Select Committee on International Relations

Corrected oral evidence: UK foreign policy in changed world conditions

Wednesday 7 March 2018

10.45 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 Purvis of Tweed; Lord Reid of Cardowan; Lord Wood of Anfield.

Evidence Session No. 7 Heard in Public Questions 56 – 64

Witnesses

I: Mr Hugh Milward, Senior Director, Corporate, External and Legal Affairs, Microsoft.

II: Dr Gianluca Stringhini, Associate Professor in Computer Science and Crime Science, University College London, University of London; Professor Maura Conway, Professor of International Security, Dublin City University.

USE OF THE TRANSCRIPT

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

Examination of witness

Mr Hugh Milward.

Q56 **The Chairman:** Mr Milward, good morning, and thank you for joining us. I am obliged to remind you and the Committee that this session is in public, and a transcript will appear afterwards that you can adjust if you think there are things in it that do not purvey the true situation. Members of the Committee must declare any interests that arise when we enter into the discussions prompted by our questions.

As you know, we are looking at a big canvas, and the paint keeps running off the face of it. It is very hard to put it together and to see the frame around it. However, we are determined to do that, and we feel that the great communications and electronic companies of the 21st century have a central part in what we are looking at.

I will start with a fairly general question, which we will follow up with a number of specific questions as we go along. Large multilateral corporations, not only but including the technology companies, have enormous reserves of financial power and enormous domination of the control of information resources, and their membership exceeds that of most nation states, as does their budget. You are potentially one of the power sources in a digital age that some idealists thought would be an age for the individual citizen, but it does not seem to be working out that way. Instead, we see vast domination of the communications system by the big companies.

What do you think is the right reaction of a big company, of which you are a distinguished member, to that situation and to the international operations of nation states as they struggle to establish themselves in these completely new world media?

Hugh Milward: Thank you for inviting me here today. Your opening question is a tough one. As a general point, there is a lot emotive language in your question on dominance and those sorts of things. Actually, I do not recognise that hugely, particularly with regard to Microsoft, our own company. We are a successful software company that is moving swiftly into services of very different kinds. I will start perhaps at that point and then cover the substance of your question.

Technologies such as the cloud, which in effect is distributed computing—raw computing power, essentially, sitting in huge data centres able to provide services to a range of different citizens in any part of the world—allow for the development of technologies such artificial intelligence and productivity tools for individuals at scale in a way that reduces the marginal cost for everyone.

For example, the development of the kinds of artificial intelligence that we think are very exciting, and we are very optimistic about their impact on the world, are now available to anyone at the kind of cost that genuinely makes them open to anyone. A decade ago, the sorts of abilities that this sort of development opened up were the preserve of the

most successful, the biggest, the wealthiest companies. The kinds of technologies that artificial intelligence and cloud computing offer democratise technology in such a way that it becomes available to so many more people across the world.

The way technologies benefit society profoundly is really very clear; they help doctors to diagnose quickly, patients to recuperate better, individuals to connect and communities to stay in touch with one another at a global level. That is the promise of technology, and I am very optimistic about how we might be able to fulfil that promise.

The Chairman: That is fair enough, but is that not slightly dodging the question? Making technology available to anyone is actually making the opportunity available to anyone to air and to promote opinions and to connect up and to influence behaviour—political behaviour, and sometimes destructive behaviour, and sometimes very constructive behaviour; you described doctors and hospitals, and new kinds of production mobilising vast areas of the world out of poverty into factories and developments that we have never seen the like of before—but it is also unleashing a lot of new patterns of behaviour. Is there not a point at which you have to ask yourselves, "If we've uncorked the bottle, are we concerned with what is coming out of it?"

Hugh Milward: There is nothing necessarily new about the development of technologies in that. Think back, obviously not to any point in our lifetimes but to the response of the Luddites to the first industrial revolution. The development of technologies gives rise to very real fears in people. It is extremely clear that any moment in the development of technologies gives rise to real fear in populations.

In the second industrial revolution, the development of the combustion engine had an impact on people whose entire livelihoods were based on horses and feeding them and clearing up after them. Those horses were literally taken away over a period of 10 to 15 years and replaced by the combustion engine. That had a profound impact on society and the way it behaved.

I accept that the way in which this fourth industrial revolution is developing causes real fear among individuals in relation to the way they see their livelihoods and their jobs and the way in which they communicate. The shift in balance that we have grown used to has now been disrupted as a result of developments such as the development of technology.

I accept that there are real fears, but I remain optimistic that we will find a new settlement and that we will navigate a path through that results in the real benefits of technology being seen by many.

Lord Wood of Anfield: I thought the analogy that you chose to draw with the first industrial revolution was really apt, because what lesson do we learn from that? We learn that companies such as the railways and the power companies become so dominant that the public have an

interest in a different regulatory approach to them. In a way, that is what the Chairman was asking, was he not?

Surely you recognise—I know you do—that the success of your company and of other tech companies has come with the consequence that you are now woven into the lives of so many people that there is a legitimate public interest in treating you differently from another successful company, and that the flipside of that is that the expectation that you act in ways that are commensurate with the impact that you have, and in particular the information that you have, and the expectation that Governments look to you to provide that information to assist in public-interest issues, are surely legitimate expectations rather that something that cramps your business model.

Hugh Milward: That is exactly right: there is a responsibility that comes with the ubiquity of technologies. You see Microsoft Word and Office on computers all over the world, and you are right: these tools are available to everyone, and people are taking value from them. Similarly with Xbox—kids are playing computer games all over the world. When we are in people's homes and offices, we have a responsibility to behave in a certain way as a global citizen. That is exactly right.

We have spent a bit of time thinking about what that looks like and how we should be behaving. I do not know whether your Lordships have seen a book that we published 18 months ago, the second edition of which came out last month. It is called *A Cloud for Global Good*, and in effect it sets out what we see as the principal tenets of that responsible behaviour and what it should look like.

It is built around three things. The first is that, as technology develops, it should do so in a way that means it is trusted, not least because if people do not trust technology they will not use it. That means that we need to be open and transparent about things like access to data and our responsibility with regard to privacy, and those sorts of things.

Secondly, the way we develop our technology needs to be responsible. By that we mean taking into account its environmental impact, its impact on communities and societies, and those sorts of things.

The third is that, in doing so, it needs to be inclusive, which means that it should seek not to leave communities behind. That has prompted further investments that we have made in technology such as TV white spaces, which in effect use the unused TV spectrum to push long-distance, high-speed wi-fi to communities that are not readily accessible in any other way. The UK is incredibly progressive on this. We also have some testing going on in sub-Saharan Africa, where it has a profound impact on communities connecting to the modern world in one leap.

Those are the basic tenets. A lot of substance is obviously attached to that framework, but we see this as incredibly important. We are thoughtful about the impact of technology, and as we develop it we are

cognisant of what it might be and seek to address the challenges driven by it.

Lord Reid of Cardowan: I do not for a minute deny the access to information, individual empowerment and opportunity brought by new digital technologies. My question is rather different and follows on from that asked by Lord Woods. I am trying to avoid emotive words and do not ascribe any motive, other than an attempt to have a successful business, to Microsoft or to anyone else, but it is undeniable, given the extent of coverage, global nature and embeddedness of companies such as Microsoft in our everyday life, that it is an immensely powerful organisation—as powerful as some nation states. However, nation states over the decades and the centuries have evolved an immensely complex system to ensure accountability, scrutiny, transparency and so on, including mechanisms such as this Committee.

I should declare an interest in that I am party to a submission to the US Supreme Court on a question of Microsoft v the Supreme Court. I do not take a side on it; I merely take the view that the matter should be for Congress and not the Supreme Court trying to apply a 30 year-old outdated law.

Having declared that, what attempts do Microsoft make, apart from outlining three areas of guidance, to emulate the systems of accountability, transparency and scrutiny that developed in the nation state? I am not suggesting that they should be similar, but given the immense power of Microsoft, Google and various others, how are their structural, organisational or systematic developments to keep pace with that power?

Hugh Milward: First, we are always subject to the laws of the land in which we operate. I am here today, because you invited me here and because as a company we have to operate within the law. That is a given. Governments are always supreme. We may be a successful company and we may operate in more than 100 countries, but that does not mean that in any respect we are above any law.

Lord Reid of Cardowan: You say that you abide by the laws of the country, but through no fault of yours the laws in different countries will be different. One country, such as the United States at the moment, may demand that you hand over information relating to a citizen of another country—say, Ireland—which is contrary to the rules of Ireland and the European Union. That in itself, your globalised power, raises huge problems.

Hugh Milward: It does, and not least for us. In a very similar way, the British Government introduced rules on surveillance that include an extraterritorial element. It puts us in an incredibly difficult position when we can have an order from the UK Government to serve data from another country in exactly the same way as in the US warrant case. That puts us in direct conflict with the laws of another country. In effect, we

are breaking the law of one country if we honour that request and break the law of another country if we do not.

The issue is not straightforward. In many respects, it is to try not to act as an honest broker but to find ways to navigate a way through. In this instance, we have been working with both the US and the UK Administrations to encourage the creation of a bilateral agreement so that you do not get this conflict of international law.

We have had a very warm reception from the UK Government, and in the US this has resulted in the CLOUD Act, which is going through Congress at the moment. We hope that such action will provide us with the legal clarity that we need so that we always operate within the law and do not find ourselves in effect in a legal no-man's land where we are damned if we do and damned if we don't. That is a good example of where we seek to find ways of always operating within the law and, where there is a conflict in the law, being able to be part of a dialogue that tries to resolve it, rather than trying to find a way to avoid it, to slip under it.

Lord Hannay of Chiswick: We have not talked at all about social media, but it strikes me, and I do not know what you think about this, that social media is now in effect completely out of control; people are writing things with anonymity such that, if you wrote them in a letter and sent them to someone, you would be sent to prison for writing a poison pen letter, a practice that was largely stamped out by effective policing.

There seems to be no way of coping with anonymous social media that contains content of a really obnoxious kind. Do you really think that the technology companies are doing enough to address that problem? A lot of this is just individuals, but organisations or Governments, when they try to interfere with democratic processes, are also using the technology to do so. There is the whole issue of what went on in the United States in the presidential election, here at the time of the referendum, in France at the time of the presidential election, and so on.

Do you really feel that the technology companies are doing enough in the sense that you have described of always trying to co-operate to deal with problems?

Hugh Milward: I should speak for Microsoft rather than for the other technology companies. The social media platform that we own—the companies are not integrated at all, but we own it—is called LinkedIn. The real value of LinkedIn is that people are in a business networking environment and do not hide behind their social media profile. The interest that it serves is the promotion of people's careers, so there is no value in any users of LinkedIn trying to hid their profile; it is a very different network.

As a general point, we too are very worried about the influence of global networks on democratic processes. One of my colleagues has just left our Brussels office to join our headquarters to form part of a new unit looking specifically at the impact of technology on democratic processes. Because

of the different nature of our social media platform, our concern is cybersecurity and cyberattacks on democratic processes and what that might look like in the middle of an election period, for example.

There is genuine worry, and we are turning a lot of attention to how we make sure that we protect those democratic processes from the globalisation of technology.

Lord Grocott: My question picks up a little on what Lord Reid asked. I will try to avoid any of my questions sounding hostile; they are genuinely not intended to be.

Hugh Milward: I will try not to be too defensive, in that case.

Lord Grocott: You have used the words "accountable" and "accountability" on a number of occasions in relation to your company, and spelled out its laudable objectives to the Committee.

I want to address the multinational aspect of the companies that you have worked for. In earlier industrial revolutions, since you mentioned them, by and large the unintended consequences were resolved, or had to be attempted to be resolved, via the nation state; if you had lots of factories, the horrible conditions had to be sorted out, which they were slowly, and the rest of it.

To whom are you accountable? A company operating largely in one or perhaps a very small number of sovereign states—they may have similar histories and comparable societies—at least has a kind of framework within which it understands it can operate. If you are operating in 100 countries, as I think you said, all right, you obey the laws in each country, but you can pick and mix.

The question in a few words is: to whom are multinational companies—let us not make it too personal and specific—accountable, and is there any democratic accountability? I am sure you will say no to this—at least, I guess you will—but do you want there to be any further bodies to which you should be accountable? A lot of people see an incompatibility—a democratic deficit, if you like—between democratic nation states and huge international organisations.

Hugh Milward: We do not elect members of our various boards, or anything.

Lord Grocott: What is the framework in which you operate, other than the framework that you define yourself?

Hugh Milward: There are a variety of ways in which we are accountable. We are obviously accountable to our shareholders and to our customers. Let us be absolutely honest: there are services that provide some sort of equivalent to Word, PowerPoint, Excel—those kinds of things—that are available for free and that users can simply download if they get value from them. Customers can vote with their feet, and they do.

We are accountable to every Government in whose jurisdiction we operate, and I would expect that if the UK Government took issue with anything that we were doing, there would be a pretty robust conversation about it. There is, and that is the right approach. We are under constant scrutiny by the press, as is right; they should be helping to hold us to account for the things that we do and the actions that we take or do not take. That is also absolutely right.

There are various mechanisms internally that we have built and that we ensure operate effectively that also provide different levels of scrutiny. We have, for example, various transparency reports: reports that go into areas of responsibility, and reports on the number of surveillance warrants that we have upheld, the number of requests that we have declined, and the reasons why—all those sorts of activities, which are very transparent.

Finally, one area which there is a lot of public concern about is the development of artificial intelligence. It is really important that we have something like an ethics committee that helps engineers to think about how, right at the beginning of the development cycle, they build in core principles on responsibility in the development of artificial intelligence, and that provides scrutiny for the way it is working.

There are a range of mechanisms in place that provide that accountability. Does that help to provide what you are looking for?

Lord Grocott: As far as is possible, yes it does.

Hugh Milward: Then perhaps I can ask whether there are any gaps that I can help to fill.

Lord Reid of Cardowan: Yes.

The Chairman: We are all bursting with new questions on this issue.

Lord Reid of Cardowan: There is one question that follows on exactly from what you said. You instil a sense of responsibility and so on, and the work is done. If you are a company, there is an annual audit. If you build a building or a bridge, there is an audit; it is traceable. If you develop a pill, you can tell who developed the chemistry and so on.

In coding, on which the whole of our society is now based, there is no similar audit process. You cannot say who changed that piece of coding at that time and why, in the event of something going badly wrong. Are you exploring that: trustable software?

Hugh Milward: This is a fascinating area and one that is developing very fast. We have a form of ownership of code that is written by our engineers, which means that if others want to use it, they pay a licensing fee. You see platforms such as Android developing that use a lot of the code that we have developed, and they pay a licensing fee for that. That is a good example of the fact that we can identify it as being written, created, by us, and we can see how it is being used.

Then we move on to areas where we have less clarity about what is going on. This is where the development of artificial intelligence is so very different from other forms of computing. With other forms of computing, you create an algorithm, which is effectively a flow. The program goes through the sequence and you get the result at the end.

Artificial intelligence is different, because the code is not written; it is a learning neural network. So a very different set of principles apply, because it is very difficult to identify who is responsible for achieving the end result. That is why we are paying so much attention to how we think about the development of this and how we make sure that we are building in ethical principles on its use and the datasets that this artificial intelligence is built on. If, for example, you introduce a bias in the dataset that feeds into the artificial intelligence, you cannot be surprised if there is a bias at the other end. So how do we think very carefully about the way we use and develop artificial intelligence to ensure that there is that kind of accountability?

This is nothing new. In the early days of the development of the car, it was very difficult to identify who was responsible if there was a crash. If a bolt sheered and resulted in the car crashing, who was responsible? Was it the manufacturer of the bolt, the assembly plant that put that piece together, the brand of the car, the showroom that sold the car, or the driver of the car at the time?

The law has clarified where that responsibility lies, and we need to get to the same point in the development of artificial intelligence so that it is crystal clear where liability lies. The entity that ends up with the responsibility, or liability, bears a disproportionate responsibility to society. Does that help?

Lord Reid of Cardowan: Yes, it does.

The Chairman: That is brilliant.

Lord Purvis of Tweed: That leads neatly to my question, but it also comes back full circle to Lord Grocott's question about who writes this. Who will provide this regulatory framework on a global basis, because this is not down to each nation state?

You will have a view on how this regulatory framework is put together. You are a massive company and you have sufficient strength and power that in many regards is greater than most of the 100 countries that you work in. I wonder whether we are in the same broad situation in which Eisenhower warned against the military-industrial complex. Now we have a technology-industrial complex: you are so large that the ability of our global institutions, which are policy-making and democratically accountable to the people, do not have the same kind of clout.

I should have thought that the institutional shareholders holding three-quarters of your shares would have an interest in cyberattacks going on, in Governments being unstable, because they will want more and more

updates of your products. Parliament had a cyberattack. What did we do? We had to update all your products. WannaCry nearly brought the NHS to its knees. What was the recommendation? To update all your products.

Hugh Milward: For free.

Lord Purvis of Tweed: That is a very good point. My question is: are the global tech companies now in effect, as we saw in the banking crisis about 10 years ago, too big to fail, because Governments are so embedded in the large tech companies' work and so reliant on them to provide services and the relationship is now so skewed that we need a much deeper process to bring in more global accountability, as Lord Grocott alluded to?

Hugh Milward: We are open to all ideas about what that might look like. We would like to be judged by our actions rather than our size. There may be a relationship between the two, but I like to think that the way we behave is responsible and increasingly cognisant of that responsibility.

Therefore the actions that we are taking are pro-societal. Any company that looks after its own interests by necessity is looking after the interests of the society it serves. Otherwise, it will not be in business for very long. You have to look after your customers, your users, the people you serve. For us, you are absolutely right: it also includes government.

We cannot think about the development of rules on technology such as artificial intelligence on our own. We would not want to even if we could, because it must involve Governments, people such as you, civic society, those who have a very different or opposing view. Without that debate, society does not reach a settlement so that it is content with the way these technologies are developing. If society is not content with the way these technologies are developing, it will not use them, which is a downward spiral for everyone.

We must ensure that civic society, privacy campaigners, open-rights campaigners, those who believe in the closing down or tightening of the internet, those who believe in opening it up, everyone, must be able to take part in the way these rules are developed. One of the best ways in which you get that representation is through democratic institutions, so we are extremely keen that Governments are the right place to make the rules under which we operate, and not make our own rules.

The Chairman: We must move on, or we will fill up the whole session with the first question. Baroness Hilton, your question comes in nicely on top of that.

Q57 **Baroness Hilton of Eggardon:** My question relates to several things that you said already, such as the democratisation of information and the problems of censorship. Authoritarian regimes are operating censorship in a way that you perhaps disapprove of, such as China. We have talked about the power of your organisation. Are you in discussion with authoritarian regimes about how they limit flows of information or use

your systems to promulgate information that is not terribly accurate?

Hugh Milward: This is an incredibly interesting question, because most Governments around the world limit in some way the amount of information that companies such tech companies use and promote. A good example of what the UK Government seek to limit is CSAM—child sexual abuse material. We work very closely with the Internet Watch Foundation and others to ensure that we are stripping the network of such material. It is absolutely right that that is taking place.

There are Governments around the world who seek to use similar mechanisms for much less positive means. There was discussion recently about how Iran, for example, is blocking the use of IP addresses used by certain social media networks, which in effect closes the use of them in that country. It puts us in a difficult position, because either we uphold the laws of the countries in which we operate, which I have already said we seek to do whenever possible, or we uphold what we might call global, democratic, open principles.

How do we navigate that? The answer is that we will try to obey the laws in the countries in which we operate, and if we find that we cannot we will no longer offer those services in those countries. There are countries that we can name here in which we have decided not to offer services because we are not comfortable with the way the Government might, for example, want access to citizens' information and data.

Baroness Hilton of Eggardon: You have a very powerful weapon in being able to withdraw your services.

Hugh Milward: Yes, we do. I would not say that we have been happy to use it, but we have used it.

Q58 **Baroness Helic:** My question is much simpler than those you have heard so far. I am of the generation that is not aggressively against technology, but I see many examples of where it can be abused. You have given some examples, cybersecurity being one area. How do you see those threats to the states, and how are you responding to them? Could you give us a concrete example of Microsoft having done something to counter a threat from either a state or a non-state actor?

Hugh Milward: I spent a bit of time in Kiev in January, leading a team investigating the impact of the NotPetya attack in Ukraine. Our concern is that too many people do not recognise cybersecurity attacks as having a victim. Too many see it as machine on machine without a strong human or societal impact. The reality is very different. They are human-on-human attacks and there is a real human cost to them.

One reason why I spent that time in Ukraine was to capture, understand and identify that human cost. We spoke to a variety of different people: the head of the President's office with responsibility for cybersecurity, and an opposition Member of Parliament who led the parliamentary ID committee. We spoke to business people and to citizens who had been affected by it, and what was really clear—

Baroness Helic: I am sorry to interrupt, but can you tell us the exact human impact of attack so that we can understand, too?

Hugh Milward: Would it be helpful if I just spent 30 seconds on what NotPetya attack was?

Baroness Helic: Yes.

Hugh Milward: A piece of accounting software that allows companies to file their tax returns with the Ukrainian Government was required in effect across Ukraine. That meant that you had one piece of software in every business's computer. One problem with the software was that it kept giving false-positive cyber readings, which meant that most people turned their antivirus off or allowed the accounting software to bypass it, otherwise it just would not work. The situation was ideal for an attack, and one of the software updates was effectively bypassed.

The NotPetya malware was installed through this platform. The malware worked for three or four days in the background before anyone knew they had been affected, and then it hit. In those four days, it spread sideways across every network. It took out around 10% of the Ukrainian Government's computers and 10% to 12% of business operations in Ukraine.

The UN has estimated the cost of it at around 0.5% of GDP—a huge economic impact. But it included real human cost. In Ukraine, digital penetration is not especially high. In countries where the digital penetration is higher, the impact would have been much higher. But it meant, for example, that doctors could not access patient records, so patients were going into surgeries and unable to have any treatment or to continue treatment.

There were irritating impacts. ATMs did not work. You could not use your bank card on public transport. You could not take out your cash or access your bank account. You could not buy anything in a supermarket. It had a tremendous impact over a 72-hour period—for some companies, for much longer. Some companies found that they could not retrieve their data. This was not one of those malware attacks where you pay some bitcoin and you get your data back. It destroyed data, so even if you paid the ransom you would get nothing back. It resulted in businesses closing, people losing their jobs, and families losing their family income.

One thing that came out of the investigation in Kiev was that there was clear evidence that this was a state-on-state attack, a Russian-sponsored cyberattack on Ukraine; the US and the UK Governments have now attributed the attack to Russia.

This kind of attack is of huge concern to us. It is one reason why we have been trying to encourage what we call the digital Geneva convention. Where the Geneva conventions protects citizens in times of war, cybersecurity attacks are increasingly being used in times of peace. How do we think about our responsibility to protect citizens in times of peace?

Our idea is to create a digital Geneva convention that sets out responsibilities for Governments, technology companies and others in order to protect from nation-state attack.

The Chairman: We are very fortunate to have your first-hand experience on this. It took out the electricity, as well, did they not?

Hugh Milward: It took out the electricity and the media. A lot of state and private broadcasters were unable to broadcast. It took out the radiation monitoring for Chernobyl.

Q59 **Lord Balfe:** I should begin by declaring that my son works for Amazon, but we have not discussed this evidence section between us at all.

I want to follow up on the interface with privacy, because one concern that came up very much last year was encryption and the inability of the security services, as reported, to decrypt the technology used by the persons who attacked Parliament, although it affects others as well.

I see that there is clearly an interface between letting Governments know what their citizens are exchanging and protecting terrorism, and it is probably quite difficult. Would you share with us your thoughts on where we could establish a boundary that would allow for legitimate interests, such as when terrorist acts are committed, but that at the same time would not be so oppressive that Governments could decrypt the messages of citizens going about their lawful business?

Hugh Milward: I do not think it is possible, to be absolutely honest. What we saw with NotPetya and WannaCry was cybercriminals exploiting vulnerabilities that they had discovered which had been hacked from the NSA. It is a good demonstration of the fact that if you create some sort of backdoor or way in to encrypted communications, it will not stay the preserve of GCHQ, the NSA or government for very long; it will emerge and then be used by criminals. I do not think it is remotely desirable to create encryption that is easily hackable or weaker or that has backdoors in it.

Secondly, encryption, being end to end by its very nature, means that the communication is encrypted from my device throughout the entire network to your device. There is no point at which the various networks that transmit the communication can decrypt it. It is encrypted at the device level. So it is impossible.

Thirdly, even if you were somehow to require companies not to encrypt communications or to make some adjustment that we have not managed to think of, people who are use those communications will simply move to another platform that has not behaved "responsibly" by reducing its level of encryption. In effect, you end up chasing criminals to the far-flung reaches of the web. It is perfectly possible for you or me to download and install PGP—pretty good protection—encryption on our computers and be able to have a conversation that neither the security services nor anyone else could access. That is available for free on open source.

The encryption genie is out of the bottle. It is undesirable to try to put it back. If you think about the number of business transactions—the City of London is a good start point—that are entirely reliant on encrypted communications, weakening or removing encryption is wholly undesirable.

The Chairman: I should like to close with a final question that brings us back to home base: the position of the United Kingdom and whether we are up to all this.

Q60 **Lord Reid of Cardowan:** Let us leave aside artificial intelligence, which you have already touched on, because we are limited in time.

How do you think that developments in the quantum field, led by those such as the Chinese, will affect international relations? How well placed do you think we are in the United Kingdom to take advantage of the opportunities and defend ourselves against the downside, or would you like to come back in writing?

Hugh Milward: I will come back now, actually, and give you a fuller response in writing.

Quantum is still some time away. Currently, it is just beyond theoretical: it is a race to get there. You are right to identify that there are profound changes to the way we need to do things as a result of quantum computing. The impact that has been broadly communicated is the fact that it "breaks encryption". The responsibility that we all have there is to make sure that there is suitable encryption afterwards at work in a different way that cannot be broken by quantum.

There are also profound benefits from quantum. The speed with which tasks can be undertaken is astonishing. In the UK, we are extremely well placed to continue the drive for the development of technologies such as quantum. We have some of the best researchers in the world, and as a result some of the most attractive conditions in which to continue to invest in the research that will allow quantum to develop at pace.

We are very worried about developments such as Brexit and its impact on the willingness of researchers who are in extremely high demand to continue to come to work from the UK, but we are also hopeful that a settlement will be found that will allow us to continue to invest in our research facilities here, and for others to do likewise.

Provided we can do that, we think that the UK is extremely well placed to be at the forefront of this.

The Chairman: And do you think that we are sufficiently protected against some of the abusive side that we discussed in earlier questions, such as stealing our technologies and our secrets? Is the UK as well protected as other countries, or do we need to do more?

Hugh Milward: From our position as a global company, the way the UK's security services operate and think about the threat environment is

pretty much second to none. The fact that the UK Government are genuinely progressive in thinking about these issues earlier than most other global Governments also puts us in a strong position to be able to think ahead of the criminals and ahead of those risks and to put mitigating or protecting functions in place sooner than elsewhere. Genuinely, our view is that the UK is as well placed or better than the next best.

The Chairman: That is an upbeat note on which to end this session. We have bombarded you with several impossible questions, as well as the possible ones, and you have answered them all with great patience and a lot of illumination. Thank you very much indeed for helping us trying to find our way through this new world. We really appreciate you taking the time and trouble.

Hugh Milward: Thank you for inviting, me and if there are any questions to which you feel that you do not have a sufficiently detailed answer, I am happy to come back in writing.

The Chairman: Excellent. Thank you very much indeed.

Examination of witnesses

Dr Gianluca Stringhini and Professor Maura Conway.

Q61 **The Chairman:** Good morning and thank you, Professor Conway and Dr Stringhini, for joining us this morning. I am sorry that you have had to wait a little, but these are huge subjects, and the questions and answers are bound to go on. We are very grateful to you for attending. This exchange is on the record, and there is a transcript afterwards if you need to change it.

We are trying to focus in a broad canvas on the way in which the enormous upheavals in technology and communication are affecting diplomacy, particularly our diplomacy here. Behind that is the bigger question of whether it is affecting the whole way in which states react to each other, the interstate model on which diplomacy is built, or whether we are finding new forces at work that upset that model completely.

First, if I may, I will ask for a general summary from both of you on how you see that broad question—whether, in fact, we are on the right track at all.

Professor Maura Conway: Thank you for the invitation. I am happy to be here.

My research has focused on two things in particular. All of it is focused on violent extremists and terrorists and the intersection between them. First, I have been interested for two decades or so now in how violent extremists and terrorists use the internet on a day-to-day basis, in particular for influence, operations and propaganda dissemination, if you like, and the potential impact of that activity.

Secondly, I have also written extensively on so-called cyberterrorism: the use of the internet for attack purposes such as on critical information infrastructures. I have always felt that the focus should largely be on the influence operations aspect. I have not had cause to change my position considerably over time, so I am sceptical about the cyberterrorism threat even up to the present, although of course there is the possibility, in particular with the internet of things, that that could change relatively rapidly.

The Chairman: Thank you. Dr Stringhini.

Dr Gianluca Stringhini: Good morning everybody. Thank you for having me here today.

In my research, I study mostly cybercrime—typically how organised criminals, non-state actor adversaries, are using technology and the internet to perpetrate crimes. In particular, I have been studying for more than 10 years the threats linked to malware and how criminals are infecting computers all over the world and organising them in botnets, so that essentially all the infected computers will report to a controller, which is accessed by the criminal and can be given orders either to perform additional criminal activity or report back stolen data, for example.

In this frame, what the internet changed is that criminals no longer need physical contact with their victims. They can certainly affect people from all over the world without moving. They can reach many more people. The advance fee fraud, for example, started a couple of centuries ago. People sent out letters promising a very financially rewarding scheme for a fee: "You've won a very large amount of money. You need to pay this fee to unlock it". Back in the day, they had to find physical recipients, write physical letters, and so on. Nowadays, they can just press a button and suddenly reach potentially millions of people. That is an example of how their reach has increased.

The other problem is that they can hide their tracks very effectively. It is often not clear where they are located or whether the control servers are where the criminals are sitting, because there may be relayers, or proxies, whereby the criminals essentially relay the connection through several countries to make it more difficult for their activity to be traced. That is from the organised crime point of view.

More recently, we have started to see more state-actor activity, which in many cases is similar. The same developments appear. People can attack victims from far away, hide their tracks and deceive attributions, so they can make it look as though it is another nation state performing the attack. Often, the two groups are not 'disjoined', so we are witnessing non-state actors collaborating with national states to perform cyber warfare, if you like.

Professor Maura Conway: In much the same way, violent extremists and terrorists see what for them are the positive aspects of the internet,

which go beyond what was previously available to them in propaganda production and dissemination at greatly increased speed, global spread, possible audience reach and cheapness. Speed, spread and cheapness are important.

Secondly, it is interesting to think about attribution in cyberterrorism, because it is a different realm from cyberwarfare. With terrorism, generally you want attribution. Terrorists largely have an interest in their attacks being associated with them.

Q62 **Lord Grocott:** Professor Conway, were you saying that digital technologies have not increased the threat of terrorist groups to quite the extent that might have been thought, or did I misunderstand you?

Professor Maura Conway: That is an interesting question. A question for researchers in this realm is: is the change that the internet has wrought more evolutionary or revolutionary? People have quite different perspectives on this. For me, of course, the dissemination of propaganda content and engaging in influencing operations is nothing new from a terrorism perspective. We often say in terrorism studies that terrorism is a means of violent communication. The communicative aspect of terrorism is very important.

For quite a long time, terrorists had to rely on the violence to speak for itself or allow it to be interpreted by third parties; generally, the media were influential in that respect. The internet takes away a lot of that mediation. Since the mid-1990s, say, it has been possible for terrorist organisations to communicate directly via the internet with their supporters—their fan communities, if you like—but also with their victims, policy communities and global publics.

I guess I am saying that the speed with which they can put out their content has increased, and the audience that they can reach is much bigger than it once was. This is quite a significant change, but the thing in itself remains similar, if you like.

Lord Grocott: I see. And what about a state's capacity to deal with it?

Professor Maura Conway: The issue here is that, until relatively recently, states had very significant capacities in this respect, because, in the past, many terrorist campaigns were really quite limited—to some region in a country, to some country, or to some small group of countries within a region. Now, the global aspects of some of these terrorism campaigns is much greater, obviously, while at the same time the ability of states to close down this information or propaganda dissemination is much less clear than it once was.

This goes precisely to the fact that, in the past, the conduit for this information was mass media. Now, as we know, social media companies and other online spaces are also very important in this respect, although it has to be said that mass media still play a significant role. But Governments' ability to regulate social media and these online platforms is simply not as great as it was for more traditional media forums.

The Chairman: You are saying that there has been a real transfer of power. The information itself is power—the power to recruit and to promote causes, good and bad—which obviously alters the challenges facing state Governments and traditional methods.

Professor Maura Conway: That is absolutely correct.

Lord Hannay of Chiswick: You have addressed very clearly what I would call the law-enforcement aspects, the criminality aspects, of this. Could you, as you go through, also address the question of whether these technical developments, this revolution technology, are affecting a Government's ability to conduct diplomacy in their dealings with other states and with the citizens of other states?

Professor Maura Conway: That is an interesting question. I did some work a number of years ago in which I considered the Lebanese Shia organisation known as Hezbollah and what at that time I called its public diplomacy campaign. This was around the time when public diplomacy was emerging as a more central issue for Governments globally but especially in western contexts.

I considered Hezbollah, but you could also consider any terrorist organisation's activity within this frame of reference, because what a lot of the groups that came to be active online from the mid-1990s onwards—the early adopters, if you like, in the terrorism world—wished to do with websites, and later forums and what have you, was to reach out to global publics and to tell their story without the mass media acting as interlocutors, because when the mass media act as interlocutors they tend to draw attention to the negative aspects of terrorist organisations' activity, unsurprisingly.

Online platforms, which were originally websites, like I say, and latterly social media accounts and what have you, allow these groups to portray themselves in the light in which they wish to be portrayed. So when I think about diplomacy, I think about the ability that these groups have developed over the last 20 years or so, which obviously poses pretty significant problems for the diplomatic efforts of various nation states.

Q63 **Lord Balfe:** We talk about governance, and terrorists and other similar organisations, but of course a key factor is the multilateral organisations: the UN, NATO and the like. Their decision-making structures make it much more complex for them to take effective action.

Do you have any thoughts on how UK diplomacy could sharpen up its act in pushing for a higher level of identification, realisation and action with our multilateral partners?

Dr Gianluca Stringhini: I will speak from the crime angle. There have been a number of multilateral operations to crack down on specific organised crime operations. I will give a couple of examples involving the drug markets. These days, there are many websites on the dark web, which is a network that is not accessible through regular means; you need specific software, essentially, to access it. A side-effect of this is

that the location of the network, as well as of the different people using it, is not known.

There have been a number of police operations to take down these services, and the UK had a prominent presence in these operations. In particular, the NCA was involved in Operation Onymous in 2013 and in Operation Hyperion in 2015. So there are already these frameworks, which typically are mediated by Europol or Interpol, and so on.

Lord Balfe: What about the more diplomatic areas? Telegrams from embassies were notoriously hacked in the late 1930s and 1940s, because the codes were broken. A lot of confidential diplomatic traffic goes backwards and forwards. To what extent can that be compromised, and what should we do?

Dr Gianluca Stringhini: That could definitely be compromised in a variety of ways. Typically, any content that is transmitted online is encrypted, so if any actor were to intercept the traffic, they could not make sense of it. So adversaries have moved on to compromising the end points. They might compromise the computers in the Houses of Parliament, say, and then perform some lateral movement, meaning that they compromise additional computers and eventually get to the sensitive data, and potentially use this data themselves later or leak it. That has been happening more and more.

The big problem from the diplomatic angle is attribution. Once the UK Government, say, realise that they have been breached, it is fairly difficult to tell who was behind it, because the difference between cyber weapons—the code that is exploiting vulnerabilities and computers—and traditional weapons is that, once a cyberattack is launched, the other party can essentially intercept your tech traffic, re-weaponise it and use it later against someone else. Wikileaks leaked alleged evidence last year that the CIA was using code from other countries to attack third parties and make it look as though another country was responsible for it.

This creates many challenges for diplomacy, because someone might suddenly be blamed for an attack that they did not commit.

Lord Balfe: Can you give an example?

Dr Gianluca Stringhini: It is difficult to attribute these attacks to anyone, but WannaCry, for example, has been attributed to North Korea, and as we just heard from the previous witness, NotPetya has been attributed to Russia. I haven't seen the evidence, but I am sure there is strong evidence for that, but in principle it is possible that these attacks were misattributed. If there was retaliation on the basis of these claims and the attribution was wrong, it would be a problem.

The Chairman: The non-attribution aspect that you have touched on is a very deep problem, is it not, because if a society's, or a country's, interests are directly and painfully attacked, as we heard in the case of Ukraine in the previous part of the session, and one cannot attribute the

source to another state, what is the answer? Is it to threaten the state that you think might be responsible, or to use conventional threats against cyberattacks? Explain to us how the modern diplomat faces this unprecedented situation.

Dr Gianluca Stringhini: This is not really my area of work; I work mostly on the technical aspects.

The information that this kind of attribution is based on should be as accurate as possible. Oftentimes, the information that we see, at least the information that is leaked to the public, is not bullet-proof. The fact that a certain attack code was used by another nation state in the past does not necessarily mean that the same nation state was behind a later attack. Let us say that the UK is attacked by a certain nation state. The attackers could collect the attack code and weaponise it again later to make it look as though a third party committed the attack.

We may look for the computers that are launching these attacks, but these computers might be infected, they might be proxies, or intermediaries and so on, so it is very difficult to tell who is behind them. So there needs to be a much more comprehensive collection of evidence before diplomatic action can be taken.

The Chairman: Without too much blue-sky thinking, is there a role for existing institutions—or for new ones, even—to try to get a grip on this problem, which every country faces, regardless of its politics, its diplomacy, its nature of government? Every country is threatened by the non-attribution problem as to where its security challenges are coming from.

Dr Gianluca Stringhini: There is a lot of discussion about this, but there has been no agreement on a solution yet. Some ideas that have been floated are essentially about regulating this kind of exploit code in the same way in which weapons are regulated, so that you cannot export them easily and so on.

However, this creates problems for the security industry at large. The security industry relies either on volunteers or on people whose job it is to find problems in software and to report them. Oftentimes, they get paid for it, and hole is closed. If it became illegal for someone in the UK to report the vulnerabilities of companies that are based in the US, the holes would no longer be fixed and criminals would be free to attack those companies and exploit their vulnerabilities.

There are many challenges, and I fear that we do not have solutions yet.

The Chairman: Professor Conway, do you have a view on what the multilateral role will be in this completely changed world?

Professor Maura Conway: I am less familiar with the activity that Gianluca has just described, and more familiar with the discussions about regulation, going back to the content again.

Over the last number of years, there has been a lot of activity in relation to violent extremist and terrorist content, and the UK has been a central player in that activity from a diplomatic and policy perspective. The UK was the first country to set up an internet unit in the Metropolitan Police—the Counter Terrorism Internet Referral Unit, or CTIRU—which alerts social media companies and other online platforms when they are hosting terrorist content and requests that they take down that content.

This is interesting if we are using an expansive definition of diplomacy, because of course all the unit can do is make a request to these companies, which can decide to proceed, or not, on the basis of that request. Numerous other European Union countries have set up similar internet referral units in the past few years, many of them modelled on the UK's. That, I guess, is one aspect of the thing.

On the multilateral level, there have been some interesting initiatives over the last number of years to disrupt this violent extremist and terrorist content. At the UN level, for example, there is an initiative called Tech Against Terrorism, which again the UK has played a role in. The Counter-Terrorism Committee of the United Nations is also a sponsor of this initiative, which seeks to alert smaller social media companies and other online platforms to the risks that they might face in oftentimes unwittingly hosting terrorist content. Facebook, YouTube and other major social media companies now have a very heightened awareness of the circulation of violent extremist and terrorist content on their platforms and are engaged in disrupting that, and have been for a number of years.

One of the upshots of that disruption is that the content is now moving to other online spaces, and terrorist organisations and their supporters have realised that smaller and newer companies do not have the same resources and capacities as the really big players, so oftentimes the terrorist content can be hosted on those platforms for some time before any disruption activity begins, if it begins at all. The Tech Against Terrorism initiative therefore seeks to educate people in the start-up community who are responsible for these other more low-profile platforms about this issue.

Another important part of all this has been the EUIF, the EU Internet Forum, in which again the UK Government has played a leading role, along with France, Germany and other EU member states. VOX-Pol, the EU-funded research project that I am the co-ordinator of, is party to the EU Internet Forum, and a lot of the activity over the last number of years to disrupt the circulation of this content on major social media platforms has been a result of the activity of the EUIF and the pressure that has been brought to bear on the major social media companies with respect to this content.

The Chairman: I suppose the question is, "What next?"

Q64 **Lord Reid of Cardowan:** Again, as Lord Hannay asked you earlier, I know this is not your area, but if I may I will ask you to look at some of the future developments in the technology and how they might affect

international relations and diplomacy, state to state or people to people.

We are aware that artificial intelligence is coming along and that the internet of things will further embed technology in all our homes and institutions. We are aware that, as the last witness said, we are on the cusp of quantum and quantum computing, so could you speculate on what effect these might have on our international relations, diplomacy and the relationship between nation states?

Dr Gianluca Stringhini: There are a number of ways in which all these technologies can be used maliciously. Luckily, adversaries have not yet found a good way to monetise and exploit internet-of-things devices. These can be wearable devices, home assistants, smart fridges or thermostats, and so on. They are all connected to the internet to some extent. So far, all the attacks that target these devices leverage the fact that they have internet connectivity. Basically, they are used as pawns in large-scale denial-of-service attacks. Essentially, the attackers send network traffic to all these devices and they will all attack a third party.

Now, once again, there could be some misattribution in the sense that a third party, let us say a nation state, suddenly sees all these malicious connections from another country, but actually this is just traffic bouncing off and it is not generated there. All these devices have great potential, because they can record videos and audio and control physical systems—think of smart locks and thermostats, as well as self-driving vehicles.

In future, organised criminals could find ways of monetising this, which could include blackmail. People might be recorded and later blackmailed about whatever was recorded. That is as well as cyberterrorism or cyberwarfare activity. Suddenly, criminals or other attackers could cause cars to crash. These are all challenges that will probably come up.

Something else related to artificial intelligence is a large concern: doctored evidence. Technology can modify the people in a video in fairly convincing ways. Essentially, strong video evidence that someone was in a place or said something could be fabricated. That could have massive repercussions if a politician, for example, was shown saying something compromising although that never happened. The question would be how we tell whether a video is authentic or not.

So far, these technologies are not perfect. They are fairly convincing, but if you look at the video there are some glitches in the way the face or the mouth move. But, potentially, they will become better and better, so it will be very difficult to say whether evidence is true or not.

Baroness Helic: Is there a country that leads in its ability to use this technology, or are we all in the same kind of space?

Dr Gianluca Stringhini: From the nation-state point of view, I am not aware of any incidents involving these technologies. I was speculating about the future. From the research point of view, a number of countries lead in artificial intelligence, internet-of-things technologies, and so on, and the UK is one of them.

Baroness Helic: When you say "future", are we talking in five or 10 years' time?

Dr Gianluca Stringhini: It is difficult to say, but in five years' time would probably be a good estimate.

The Chairman: I am going to ask a final question that it was probably rather pointless asking our earlier witness.

When oil began to dominate the world economy, and Standard Oil began to dominate oil, became the overweening monopoly, shaped the whole motor industry and created many other consequences, the reaction of the political world and the public was to break up the monopoly, which was done with tremendous ruthlessness in the United States.

Now we look at what appears to be a set of vast monopolies dominating the information system of the globe. Is it practical to think in terms of breaking them up?

Professor Maura Conway: Clearly, there is a relatively small number of social media platforms in particular that have dominated where my interests lie: with the circulation of violent extremist and terrorist content. Many people ask me where I find this content. Sometimes they have in mind that I have to dig very deeply online. In particular, people think that this content must be available only on the dark net or in other shady corners of the internet, but of course until quite recently, even very explicitly terrorist content, such as the content produced by the so-called Islamic State, was very easily available on really major social media platforms: in particular Facebook, which truly dominates, but also Google's YouTube, and Twitter.

Another aspect was that, for some time, the response of those companies to the circulation of this content on their platforms was not what many Governments and policymakers thought it ought to be. In fact, there are Governments and policymakers who still do not think that the response is sufficient.

Having said that, as I already mentioned, for the past few years there have been relatively frequent contacts between Governments, particularly in the European Union space with the European Union Internet Forum. An important part of that forum is that the social media companies are parties to it. Latterly, the Global Internet Forum to Counter Terrorism has been established by the big five—four major social media companies and Microsoft. I would say that that has come directly out of those contacts and the negotiations with EU member states in particular, and from the social media companies' realisation that they would have to respond more convincingly on this issue than they had been doing to date.

Lord Reid of Cardowan: On this question of counterterrorism, countercriminality, or whatever, we tend to look at atomised risk, at one technological development. Have you, in the course of your studies, given any consideration to combinations of risk? What I mean, bluntly, is that

we are all now used to drones. We now know that facial recognition can pursue you from a drone. Viral warfare is now very much in the news. If you put those three together, it is quite a frightening combination. Have you given any thought to that, or do you know people who have?

Professor Maura Conway: I guess that, from my perspective, one thing that is underrated with regard to so-called Islamic State and its successes, which I think goes somewhat to your question, is that the conflict in Syria is very much a hybrid conflict. If we consider Islamic State as just one of a very large number of players in that conflict, a very important part of all this is obviously what is going on on the ground in Syria and its involvement in that.

Then there is the terrorism piece, which in a western European context is what concerns many policymakers. Then there is the really significant online piece. Since the establishment of its so-called caliphate in the summer of 2014, those three things have all come together in such a way as to give it a very high profile as actor in that conflict and in the terrorism space more widely.

Often we put significant emphasis on the online aspects, and my particular research interest is in that, but an important part of its "success" has to do with the nature of the conflict that is ongoing on the ground in Syria, in conjunction with the terrorism piece and the online aspect. It has had significant "success", from its perspective, with the development of its online strategy, but at the same time it has made significant strides in other technology areas. For example, it has developed a variety of improvised explosive devices that it has employed on the ground. You mentioned drones. It is also a relatively heavy drone user, some of which activity we can witness in its online content and videos that it has circulated.

Lord Reid of Cardowan: And now with facial recognition a drone can target and follow you.

Professor Maura Conway: Correct. In a more general way, over time we have often witnessed a trend whereby technologies utilised by nation states are utilised by terrorist organisations; they learn by the activities of nation states. Nation states are now using drones and other technologies. The past tells us that we can expect other actors increasingly to think through how they can use them.

For a very long time, I was sceptical about cyberterrorism. I remain somewhat sceptical for reasons of attribution and the "bang for the buck" aspect. For example, taking down the power grid could be conceived as accident, which does not make for "successful" terrorist attacks. But changes such as the internet of things probably mean that there will be many more avenues of risk that can be exploited by terrorist organisations. We already see cyberattacks being carried out by other actors below the state level, so we might expect this to prove to be attractive to terrorists.

I do not think it is attractive in the short term, because we have seen that very low-tech, very cheap attacks have been successfully crowdsourced, if you like, by so-called Islamic State in particular. Its supporters have carried out vehicle attacks and other types of attack that are very cheap to carry out and very low tech in their nature but that have resulted in massive exposure and increased levels of fear in western and other countries.

Given that that is possible, cyberterrorism is potentially much more complex and much more subject to failure from a terrorism perspective, so it is probably not as attractive as people might think it is on the face of it.

The Chairman: That is a fascinating comment. Mr Stringhini, do you have a final comment to make on that area?

Dr Gianluca Stringhini: Yes. From the point of view of organised crime, criminals are already using multiple technologies in conjunction with each other. In particular, we are witnessing single criminal actors specialising in a specific step within the criminal operation, such as solving captures, which are those weird-looking sentences that computers should not be able to solve, or being sure to install matching malware on a mobile phone and on a computer that belongs to the same person, which can defeat two-factor authentication, and so on. Every time there is a new technology and a new opportunity to monetise it from a criminal point of view, someone will specialise in it. We are already seeing that.

A challenge with newer technologies such as drones, the internet of things and so on is that criminals have to figure out a way to monetise it at a large scale. This is what is slowing down the adoption of these technologies by criminals at the moment, but I think it will happen in the future.

The Chairman: That has shown us a glimpse of the future. We will have to leave it there, because we have run out of time, but we are very grateful to you for helping us on our way through this tangle of new complexities and are most grateful to you for your insights. Thank you very much, Professor Conway and Dr Stringhini.