House of Commons

Foreign Affairs Committee

Oral evidence: Tech and the future of UK foreign policy, HC 201

Tuesday 29 June 2021

Ordered by the House of Commons to be published on 29 June 2021.

Watch the meeting

Members present: Tom Tugendhat (Chair); Bob Seely; Henry Smith; Royston Smith; Graham Stringer; Claudia Webbe.

Questions 1 - 50

Witnesses

I: Ria Thomas, Managing Director, Polynia Advisory; Harriet Moynihan, Senior Research Fellow at the International Law Programme, Chatham House.

II: Toomas Hendrik Ilves, Former President of Estonia; Ashish Jaiman, Director of Technology Operations, Microsoft; Hugh Milward, General Manager, Corporate, External and Legal Affairs, Microsoft.

HOUSE OF COMMONS

Examination of witnesses

Witnesses: Ria Thomas and Harriet Moynihan.

Chair: Welcome to this afternoon's session of the Foreign Affairs Committee. We are very lucky to have for our tech inquiry this afternoon two very impressive witnesses in our first session. Ria, will you introduce yourself?

Ria Thomas: I am Ria Thomas, managing director of Polynia Advisory. Polynia advises large global firms on looking at cyber as a holistic risk. My perspective today will be rooted in advising over 25 global firms as they have dealt with large-scale cyber-crises with cross-border implications. I look forward to our discussion.

Harriet Moynihan: I am Harriet Moynihan, acting director in the international law programme at Chatham House, otherwise known as the Royal Institute of International Affairs.

Q1 **Chair:** Thank you, both of you. Perhaps I can start with you, Ria. Where are the current gaps in international law in global technology governance, particularly in terms of specific technologies or their applications? What might be the consequence of failing to address these gaps?

Ria Thomas: This is something that I am sure Harriet can fill us in on as well. With regard to the gaps, it has been well documented that current international policy or law is not sufficient, but attempts have been made—for example, the recent consensus report by the open-ended working group at the UN is a definite step forward in terms of at least looking at some of these key issues. But the reality is that we are a few years away at best from being able to implement what the details are. In the meantime, where the challenge lies is with regard to how nation states are creating their own regulatory frameworks on a range of issues related to technology. They might not necessarily be aligned, and they have broader implications, especially for companies here in the UK.

I can give you an example of what I mean. Let us look at data protection as an example. With data protection, I know the UK's ICO, for example, is closely collaborating and co-ordinating with other allied Governments. The reality, though, is that if you are a large global firm and you are in the middle of a major data breach that has multiple implications in multiple markets, you are now having to notify regulators—in the case of one of my clients, it was well over 85, but in some cases it is over 100, depending on how spread out they are geographically across the globe. As with any crisis, the challenge is time. In a cyber-crisis, there is not always time to be able to not only notify all these regulators but to be able to meet the obligations you have to others, such as your customers or your partners.

The challenge is how exactly—in the interim, before international frameworks are agreed—we streamline some of these regulatory frameworks that exist, whether that is on a bilateral or regional level, or also with what I would consider to be traditional adversaries. The reality for global companies, including ones headquartered in the UK, is that they don't just operate in the UK or Europe or in allied countries; they are in markets that are much more challenging for them. What is it, from a foreign policy perspective, that can be put into place or at least understood by the Foreign Ministry that would mitigate some of the issues that might arise?

Chair: Thank you very much. Harriet, did you have anything to add to that?

Harriet Moynihan: I would say that international law does not have gaps in itself—international law applies in cyber-space, and that has been agreed by the UN and many states and international organisations. The problem is how it is applied. I would agree with Ria that it is taking some time to have a full understanding of how we apply international law, for example, in cyber-space. In the meantime, we see the proliferation of cyber-attacks and other problems that Ria has highlighted in relation to a lack of harmonisation around data and data free-flow.

Ria mentioned the issue of how we mitigate the fact that it is very hard for the law to keep up with technology that is fast evolving. One mitigation strategy that I think states and other actors are increasingly relying on is soft law. When we think about hard law, we think about treaties, binding on states. Soft law we might think of as politically binding, but not legally binding. For example, it might be principles or an MOU or norms. In the cyber context, Ria mentioned the open-ended working group, and there is a group of Government experts at the UN trying to thrash out how international law applies. In the interim, there has at least been agreement reached on 11 cyber-norms, which have quite a lot of relevance to cyber-attacks.

One of them, for example, is that states should not knowingly allow actors to commit cyber-attacks from their territories. It is almost like an obligation of due diligence. While that is just a norm and is not legally binding, increasingly it has encouraged certain states to come out and say that they do actually think that that is legally binding—that there is a duty of due diligence. We not only think that soft law is useful as an interim measure, but it can ultimately concretise into hard law.

The other valuable role of soft law in this context is that, as we know, technology regulation requires not just states but the involvement of non-state actors, whether it be private companies or civil society. The benefit of soft law is that it enables the participation of non-state actors. I would just give one example there of the Christchurch Call, which is states and tech actors working together on the regulation of extremist content online.

Q2 **Chair:** That is interesting. You seem to be building up. I don't know if you have read histories of piracy and the pirate wars of the 1700s and 1800s. It was that building up of the soft norm; first of all, you don't sponsor pirates, then you don't tolerate pirates and then you actually fight pirates, and that led to the end of piracy in the 19th century. Well, the end of major piracy.

What are the risks of failing to establish these norms, Harriet? You have spoken about how they can be built up. What are the real contentions—what are the pitfalls that we could come to? What are the greatest areas of contention between countries?

Harriet Moynihan: There is a geopolitical issue in terms of very different approaches to technology regulation. For example, we are seeing a real trend of digital authoritarianism, especially in Asia, but in other parts of the world as well, which has really increased under covid. For example, there has been a rash of laws that have given Governments control over social media, there has been a greater emphasis on surveillance, and internet shutdowns are also on the rise.

Although we may have democratic countries increasingly forming alliances on technology governance and having an open and global democratic approach to tech governance—we have seen that coming out of the G7, for example, and the OECD—on the other hand, we have this risk of a splinternet effectively emerging because of a very different, authoritarian approach to tech governance. Technology and the way it is governed is not neutral. Values do matter, and I think that is one of the difficult areas that the FCDO and other Government Departments are wrestling with at the moment.

There are, however, some quite interesting middle states, or what we sometimes call digital deciders, who have yet to really set out their stake in terms of which approach they are going for. I think that there is real scope for the FCDO to have a dialogue and to form partnerships around the value of an open and global approach to governance and to the rules on that, drawing potentially on its own models, which might include, for example, the Online Safety Bill, although it is still embryonic.

Q3 **Chair:** You have covered a lot of the points that I was going to raise, so I am extremely grateful for that. Is there an appropriate level of Government interaction with the private sector? There is a degree of liberty and a degree of privacy, of course, that we have to look at. Ria, perhaps you could give us some thoughts on that.

Ria Thomas: Yes, you are right, but one of the things that I find interesting is that, in these discussions about technology governance, the perspective and the lens that is currently had when Government are looking at this appears to be still very technical. What I mean by that is looking at the opportunities of technology, the vulnerabilities of technologies, and the responsibilities of technology companies. The reality is that, these days, every company is a technology company; it is not just that sphere that needs to be looked at.

If we are going to get to a stage where there is more consensus related to whether it is norms or ultimately hard law, it really needs to be more widespread as to what exactly is the impact on broader society. That cannot be understood by simply looking at the technical piece of it, but by looking also at how non-technology-based companies, and the disruption or misuse of technology on their behalf or against them, ultimately leads to further breakdown in terms of societal impact. I think the only way we can have broader consensus, if you will, is to have more voices. By that I mean not just technology companies, but non-technology companies as well.

Q4 **Graham Stringer:** This is really a follow up to the points that you made. Harriet, have there already been practical examples where international law has fallen short? What have the consequences of that been, and are there any impending crises that we should know about where the law is unlikely to catch up with current practice?

Harriet Moynihan: One area that strikes me as difficult, particularly for international law, is the regulation of disinformation. It is a real problem, both in terms of foreign actors conducting information operations and, increasingly, as a domestic-driven issue—and sometimes they are mutually reinforcing. If we look at, for example, electoral interference, which we saw in the 2016 US presidential election, there was an emphasis on bots. We could maybe try to regulate bots, but the techniques for disinformation have rapidly moved on to deep fakes and the use of influencers.

Where international law tries to analyse it is in terms of the debate around what is mere influence versus what is actually an illegal action. I think there has been a real struggle to get to grips with that issue, and because it goes to the heart of democracy and the society that we have it is a very important issue for us to regulate.

We are starting to see some efforts from the European democracy action plan. The EU has come out with some thoughts on regulation, which I think are valuable. We are also seeing tech companies come out with self-regulation. Facebook and Twitter, for example, have a policy on foreign influence operations and we are seeing civil society play its role too, with fact checkers.

I think this is something that we are going to see potentially get worse. It is very obvious that certain foreign actors are really very sophisticatedly involved in many democracies in trying to weaken them. That is one area that I think international law is currently really struggling with.

There are a few other areas where I think international law may need updating. Quickly, one of them is outer space. We know that outer space is increasingly crowded. It is not an area that I lead on, but the 1967 outer space treaty is in desperate need of updating to deal with things like potential cyber-attacks in space, mini satellites and various other activities, both by states and non-state actors. A lot of states are aware of these things but, as Ria said at the start, the problem is the time lag between initiating these big debates between states and the rapid evolution of tech in the meantime.

Q5 **Graham Stringer:** Can we draw the conclusion that democratic

Governments are not being proactive or aggressive enough in that area?

Harriet Moynihan: I think we always feel like we are reacting, because of the tech, but in fact I would say that some states are now being very proactive, and I would count the UK as one of those. Look, for example, at the G7 with its digital agenda. Many good things came out of that, with the road map and co-operation on data standards, and technical standards as well—all sorts of things.

A new Administration in the US is open and keen to look at tech regulation, and the EU, Japan and other like-minded states are starting to form strong transatlantic tech alliances. We have the EU and the US with their Trade and Technology Council, and the OECD is doing a lot of work on, for example, the responsible principles of AI.

Those things might seem, again, to be rather reactive, but what is interesting is that we are starting to see some anticipatory features. So the EU Digital Services Act and the UK online harms Bill are deliberately trying to future-proof themselves in a number of ways—for example, by using codes of conduct that are quite nimble and can be adapted and changed quite quickly if technology changes, and a systems-based approach, rather than a linear, mechanistic approach, to policy making. It is early days, but we are starting to see a more proactive approach.

Q6 **Graham Stringer:** If I can turn to Ria, I understood you to say that individual countries were taking initiatives that were not really integrated. Beyond that point, is there the likelihood in future of a global split into two different regulatory systems—one based roughly on the Americas, Europe and democracy, and one heavily centred on China?

Ria Thomas: Sorry, do I see that continuing to happen?

Graham Stringer: Do you see that as the future—that there will be two almost completely separate regulatory regimes?

Ria Thomas: I can see the potential for that. The reality is that, at this stage, it is still early enough for that to be, not necessarily stopped, but understood in terms of what some of the implications are. Perhaps I can give some practical examples. Forget the "adversarial nations versus us" point of view alone, but look at how even some allied nations can be challenging, depending on the rules they come up with.

You might be aware that, in the past couple of years in particular, companies have been dealing with ransomware attacks. These are attacks that basically shut down their operations, or take heavily business-sensitive information, and holding it for ransom. That is one of the biggest challenges that executive boards face.

The reason I raise that is that, if you are a company that has been down for several weeks, is being threatened to be sued by your customers, partners and so on, and is in the process of being encouraged by your insurer to make the payment, then if you are a UK company with significant US market interest, you now have a new wrinkle. In October

2020, as you might be aware, the Department of the Treasury came out with guidance that any company that pays a ransom to an individual or individuals within a sanctioned jurisdiction has to face civil penalties and/or even potential criminal liability. So here is a like-minded country with a well-intentioned approach that has implications for how these approaches are changing and evolving.

To answer your original question, do I see that splitting? Of course, there is currently a tug of war between different points of view about these issues, and about the underlying freedoms, depending on how one views it. At the same time, in the inner rim, there is an even more nuanced struggle, especially for UK interests, in terms of what choices companies are now facing, even within a sector that has a united front. That is one example of some of the challenges that exist, even in the current framework. That will only get worse as we move towards an even more bifurcated system.

Q7 **Graham Stringer:** Finally, if you think negotiatory treaties are partly the solution to some of the issues and problems, what would be your advice to the UK's Foreign Office about how to approach these negotiations? What partners should they be operating with and where should they look for new advice?

Ria Thomas: It is incredibly important to keep engaging with the technology companies. There are a critical element of the ecosystem. But at the same time it is just as critical to engage with civil society, academia and non-technology companies. The reason is that there are implications that are not always apparent. It might be helpful to speak in concrete examples, just to explain why it would be helpful for the FCDO and foreign policy makers to really understand where the implications are and how they may be able to engage not just in terms of what the technology is, or its use or misuse, but what the practical implications are.

One example is insurance coverage. Let me explain what I mean by that. If the UK at one point decides, in the case of an attack against a company, that it will hold a third country accountable and say that this was a political act of war, the company's insurance coverage would no longer apply, because of the war exclusion. At present, there is a grey area as to who would cover those damages. Should there be, at the national level, a reinsurance scheme similar to terrorism, where the Government would step in? Or, at international agreement level, as the discussion towards enforcement starts to happen, should countries who are technically held accountable face accountability in terms of reparations not just to the country but to the private sector companies that have been targeted in the act of war—for a cyber-attack?

The reason I mention that is that the more the FCDO interacts with companies that are sitting across multiple spaces and multiple industries, as well as academia and so on, the more this will give a layered, nuanced approach to what exactly the policy issues may be that come up in the future.

Q8 **Bob Seely:** If I may, Chairman, I will continue with your piracy model. My first question to Ria and Harriet is whether the big problem here is the state-sponsored cyber-piracy and cyber bad behaviour, or is it the non-state stuff? Politicians tend to talk about Russia and China. Are they the significant problem here, or are we over-focusing on that?

Ria Thomas: That is a complex issue. First of all, yes there are non-state actors that are thriving in this space. Especially with covid-19 and remote working, the attacks that companies have come under are not purely nation-state attacks. The broader challenge in terms of non-state actors and the law and the ability to hold them accountable once something is attributed to them—that may exist under current national law or even agreements that exist—is going to be when you have a nation state that is behind it, because that triggers the political aspect and decision making that needs to take place.

One other example that I can share is something that I see potentially coming. If a company comes under a nation-state attack, often the Government are involved in the investigation. Most likely, that investigation would be classified. If it is classified, the company then has a very limited opportunity to speak out about what has happened and provide information to the other stakeholders, whether the shareholders, partners or customers. To your own Government's regulatory authorities, you might be able to provide classified briefings or notifications, or even to your allied countries, but what if you are operating in multiple markets where the UK does not have a close relationship, or has an adversarial one? As a global, UK-based company, what are you then facing? The challenges that you face when it is a nation-state attack are very real and are actually more in the grey area than if you are facing non-state actors.

Harriet Moynihan: I agree with Ria. I think there is a mixture; sometimes it is a state, and sometimes it is a non-state actor. International law envisages the situation where a non-state actor is under the direction or control of a state, and then that attack could be attributed to the state and that could be a violation of international law. So, increasingly, we are seeing states using non-state actors as proxies, but international law can cater for that situation. If so, if there is a violation of international law, that gives the target state a range of options, including, potentially, countermeasures, as well as legal measures, such as expulsion of diplomats and sanctions.

Attribution is very important. Ria alluded to the fact that you can have an attribution that shows that it is a violation of international law, or you could just attribute it to a non-state actor, where there will not be so many options under international law. But in order to attribute, you really do need to see Governments and the private sector working together. The private sector plays a critical role on the technical side, so it is a really good example of the importance of the partnership.

Q9 **Bob Seely:** But, Harriet, this is the basic problem. It is all very well us saying that this soft practice will eventually mould into something harder and we can get rid of cyber-piracy and cyber-attacks and everything that is bad online. The reality is we can have all the laws we want, but if there are major states like China or Russia that either accept this privateer bad behaviour online or, in fact, actively encourage it through cyber-attacks, by testing our defences, whether it is in nuclear power stations, media institutions and so on, there is not really a lot that we can do and we are stuck in, effectively, a battle for cyber-supremacy between these two significant entities: a democratic world and a non-democratic world. Do you think that is too binary?

Harriet Moynihan: I feel that there is more nuance there, and it arises from the increasing debate about how states see international law and states actually backing their understanding of attribution and the other rules that automatically apply—those international rules do apply in cyber-space. A group of Government experts recently published in its report an annexe of national positions, with states coming out with their views on how they think the law applies, which is increasing granularity about the law. It also, in a sense, creates international law, because international law is partly based on what states think is legally binding on them.

I think there is some force in this whole naming and shaming. If you can call out a state for having carried out a cyber-attack, and not only call it out for doing so but say that this is a violation of international law, that does have some force. We see that by the fact that, often, states will deny that they were responsible, because they do not want to be seen to be an irresponsible power.

Q10 **Bob Seely:** So you think trying to work with people is probably better than showing them up, but do you need a carrot-and-stick approach?

Harriet Moynihan: I think it needs to be a smart mix of both, and that is where alliances come in. We are seeing, increasingly, this collective attribution, which is much more powerful than states doing it on their own.

Q11 **Chair:** I am just going to come back to questions about public-private partnership, because, clearly, one of the big challenges we have in the world as we go forward is setting standards. There are various obstacles to this that various people have identified in written evidence and in articles. It is everything from agreeing the basics of what the basic principles mean, to getting international agreement on them. How do you see those obstacles, and how do you see the role of an organisation like the Foreign Office in overcoming them? Ria, perhaps you would like to start.

Ria Thomas: I think the Foreign Office would play a critical role, and part of it is really raising awareness. What I mean by that is that, often in standard setting, I have started to notice this technocracy-based approach, where it is individuals with a technical background who are involved in the negotiations and so on. That is very helpful, but at the same time, because of the broader implications, it is really important that this be a broader approach across the FCDO, as an example, and that any FCDO representatives or the diplomatic corps have an understanding not just of what the technology and its uses are, but of what the implications are.

In terms of what I mean by that, to go back to the point Harriet was making earlier about attribution, I do not know if this is already part of FCDO training, but it would be helpful to have an understanding of what some of these challenges can be, whether it is technical attribution and then what that means in terms of political attribution. I use that as an example to say that, when it comes to standard setting, it is really important that the individuals involved are not just people with technical backgrounds, but people who have a broader sense of what these issues are. Part of that is not just training; it is also actual engagement with the private sector.

One of the things that I have had an opportunity to do in the past, which I found very interesting, was to facilitate a roundtable between the executive board of a company and all the Government stakeholders that would be involved in a large cyber-crisis response. For this particular country, it involved not just their Defence Ministry, emergency data protection and industry regulators; it also involved the Foreign Affairs Ministry. Initially it was very confusing as to why the FCDO equivalent was there, but through the crisis simulation that was done, it became very apparent that, when it came to broader policy making, it was helpful for the FCDO-type entity to understand how all these various issues came into play bilaterally and in the multilateral setting.

To answer the original question, it is making sure that there is an opportunity for the FCDO to be more broadly involved in understanding the implications and then trying to future-proof where some of these issues may come from.

Chair: Harriet, what do you think?

Harriet Moynihan: I agree with Ria's point that there needs to be a broad set of actors talking about these standards. Civil society organisations have found it really hard to get to these standard-setting bodies. There are often barriers around cost, the high level of expertise and the time. But I do gather—I have heard this in meetings before—that the UK's national delegation has taken civil society experts and industry body experts with it to inform its view. So the UK is actually quite a good leader in this, and other Governments should be doing the same—having this multi-stakeholder approach.

The reason I flag up civil society in particular is that, as you may know, Chair, there are proposals from China at the moment to industry standards bodies like the ITU for a new internet protocol. For too long, the technical community has been aware of these, but the broader community has not been—that includes the human rights community, but also some Governments. Having that civil society perspective to really understand some of the societal effects of these technical proposals for the internet and state control is especially important.

Q12 **Chair:** You raise some interesting points there. One of them is the ITU element and the way different standard-setting bodies have imported, quite understandably, the norms and the cultural influence of the organisations, or rather the individuals that lead those organisations. In the ITU case, the Chinese leadership has naturally brought with it an understanding and perspective of the world through Beijing's eyes. It is hardly surprising—we all bring our own perspectives with us. How do you see these challenges to standard setting, with it being, effectively, localised—having much more of a local imprimatur? Maybe all I am asking is, how different is this from the present western imprimatur?

Harriet Moynihan: Sorry, I don't quite understand that question.

Q13 **Chair:** At the moment, most of the standard setting in international trade has been based on the fact that, at various points, the Dutch, the British, the Europeans or the Americans have standardised international trade. Your point about the ITU is that other nations are now having their input—in this case, China. How much of a challenge do you think that is for the new tech standards?

Harriet Moynihan: I think it is a challenge in that some of the technology is moving very fast. To date, from what I gather, sometimes representation from the UK and other Governments has not been as solid or as numerate as it might be. There has been a lack of representation on these issues. I think it is now fair to say that there is a much better understanding that these standards are by no means neutral—they carry with them their own values and approaches to how the internet is regulated. Therefore, there is a real push to get much more of a multi-stakeholder approach, so that this is not dominated by either western countries or China. It should be something that the whole of the community works together on, including the private sector and civil society and also standard-setting bodies. The ITU is not the only body. There are many other international standard-setting bodies. Some of those are developing their own human rights protocols. It is good to see that there is a lot more attention on a broader perspective than just purely the standards themselves in a technical sense.

Chair: I know that you have to leave in about five minutes, so forgive me for keeping you. Claudia, did you want to come in?

Q14 **Claudia Webbe:** I just wanted to touch on one issue. Governments are not perfect. We have Governments across the world that are increasingly authoritarian. We also have civil society that often wants to be part of the agenda of how technologies are established, but that, as has been indicated, does not have the same power bases. Then, of course, we have the private sector operators. How do we create something that is more just and fair?

Ria Thomas: That is a very difficult question to answer in terms of how one creates what can be a more just and fair approach. It goes back to how we create pathways of engagement with non-traditional partners. Harriet made a point about civil society. I raised a point earlier that this needs to be broader even within the private sector. We need to look at this as a broader societal issue.

Technology underpins every aspect of our society these days, so we really need to start identifying who those stakeholders are. They are not simply one type of company or one type of demographic. It is trying to figure out what that balance ought to be. To me, that is a broad range of voices, similar to the types of witnesses you have asked for evidence from, including written evidence. That will give a broader perspective about what issues are currently not being addressed and maybe nuances to certain topics that might not exist if only one or two voices dominate the discussion.

Q15 **Claudia Webbe:** Harriet? Where we have increasingly authoritarian Governments, we can create global standards, but we have seen where Governments have intervened to close down whole spheres of technology, simply because they did not meet their agenda.

Harriet Moynihan: Thank you for that question, which is very germane to a lot of the work we are doing at Chatham House. What is the future of global governance? Echoing Ria's point, how do you bring in the different stakeholders? We maybe need to recalibrate some of the international institutions so that you can enable contributions from civil society, who can talk about the things that you are saying in terms of internet shutdowns and authoritarianism. Responsible business is also a really valuable voice for the future on tech governance.

The key to trying to push back against the shrinking civil society space that you are talking about and digital authoritarianism is alliances. While we have lots of alliances in terms of states, like the G7 and the OECD, we also need multi-stakeholder alliances. A lot of these western companies, like Facebook and Twitter, are operating in very difficult situations. Twitter has just been shut down in Nigeria. There are a lot of clashes between Facebook and Asian Governments where there are real tensions about how much freedom of expression there should be online.

If people are buying into the same values approach that is being pushed out, for example, in the UN Secretary-General's "Roadmap for Digital Cooperation"—not just Governments, but also private sector and civil society—that is much more powerful. It is not a quick solution, but it is something that we are really trying to build on, thinking about ways to involve not only western states, but the global south, and have a much more multi-polar approach to tech governance, based on the same values, where we can.

Q16 **Chair:** There is a real question here about how the FCDO works to build these things together. The challenge is not just that there are different organisations, because Lagos, for example, has a very vibrant tech sector with an amazing number of entrepreneurs, but it has very little access to the governance mechanisms. What can the FCDO do to help that?

Ria Thomas: I think this might be something that Harriet is more familiar with. To give my two cents on it, I think, again, that it goes back to the engagement piece. Before you can engage, there needs to be an awareness for the FCDO representatives about what these issues are. I am not sure, at this stage, how widespread of an awareness there is. Before we can talk about what the ultimate solution is, it is really about laying the building blocks to say, "Is there an understanding of what the issues are? Do we speak the language that allows non-tech people to speak about these issues in a way that is about broader policy making in this space? What does engagement actually look like? Is it outreach programmes? Is it development schemes?" Again, these might be ones that Harriet has more details on, but from my perspective, it needs to start with a broader base level of understanding and work from there.

Harriet Moynihan: I agree with Ria, as ever. I think that there is a need for capacity building in some of these places because, as you mentioned, Chair, not all states have the same capacity, and that is something that needs to be built up and discussed from a values perspective and from a cyber-security perspective too. I understand that there are already capacity-building programmes going on—not just from the UK, but from the EU, the US and other countries—thinking about really selling the benefits of an open, global approach to tech, in terms not just of human rights but of the huge economic benefits for profits and innovation versus a sovereignty and control model. Essentially, internet shutdowns are not a good thing for business.

One idea, to come back to Ria's point about how much Government actually knows about tech, is the Future Tech Forum that the UK has launched, which will start up in September in London. It is seen as a sort of brainstorming of multiple stakeholders—private sector and policy makers—to think about how we push forward a common vision over a five to 10-year framework. I really like that idea, and I think there is some momentum behind it at the moment. The FCDO obviously needs to work with DCMS, which is heavily engaged in this digital agenda and is already involved in quite a lot of international dialogue, to make sure that it has a joined-up approach.

Q17 **Chair:** One of the recommendations in the "A brave new Britain" report that we published a little while ago was that the UK have a tech envoy, specifically to larger tech companies. It sounds like one of the things that you think would be relevant would be for us, and certainly large high commissions or embassies, to have a tech representative who can feed in, or at least collect, ideas for tech standards from the country in which they are based. Do you think that would be a good idea?

Harriet Moynihan: I do think that is a good idea. Of course, the interesting flipside to that is that Microsoft has opened its own representative offices at the UN, in a sort of Government-style way. I think those sorts of increasing partnerships are very important. I would just make the obvious point that the private sector has its own agenda always, so it is important to balance that voice with civil society and other actors. Certainly, it is a good way of ensuring that Government are up to speed on tech developments, so I would support it.

Q18 **Chair:** Ria, do you have any last points? I know you have to go, so I am sorry to keep you very briefly.

Ria Thomas: Not at all. Just to add to that, although I do believe, as I mentioned earlier, that the tech envoy approach is a very useful and helpful one, my concern is that, at this early stage of this type of standard-setting, we are making it into very much a technical issue, and I really think that, at any embassy worldwide, there needs to be a broader understanding among the diplomatic corps about what the use and misuse of those technologies means in terms of the broader economic and societal impact. That cannot be reliant just on the tech side of things.

Chair: Thank you very much. You have been extremely generous with your time. I have gone a few minutes over what we agreed, so please forgive me, and I will very happily release you to get on with your afternoon.

Examination of witnesses

Witnesses: Toomas Ilves, Ashish Jaiman, and Hugh Milward.

Chair: I welcome our next panel. If I may, I am going to ask that you introduce yourselves in the same way as the others did. Mr President, it is very good to see you again. Thank you very much indeed for doing us the honour of attending this hearing, and the same to Mr Jaiman and Mr Milward. As before, I can address you how you choose. Is Mr Jaiman and Mr Milward okay? Mr President, if you have any changes that you would like, please say so. Please introduce yourselves with your name and current position, then we will go straight to Royston. Perhaps you could start, Mr President.

Toomas Ilves: I am Toomas Ilves. I was President of Estonia for 10 years. Probably more relevant is that I started the digitisation of Estonia in the early ’90s and that I have been involved with cyber-security ever since the early 2000s, including the massive shutdown of my country in 2007.

Ashish Jaiman: I am Ashish Jaiman. I am the director of tech ops in the customer security and trust organisation at Microsoft. In my role, I help customers to improve their cyber-security using data analytics and AI. Lately I have been working on disinformation, the deep fake issue, threat modelling and potential compromises.

Hugh Milward: I am Hugh Milward—please call me Hugh. I am the general manager for corporate, external and legal affairs for Microsoft in the UK, and I have responsibility across all those areas. Most recently I have been working on yet another one of our cyber-attacks that we have been facing from a nation-state actor.

Q19 **Royston Smith:** Thank you, all, for joining us today. We are all very grateful to you. In what ways do new technologies, such as AI and machine learning, social media or cyber-capabilities, present a threat to democracy and the values of the UK and its allies?

Toomas Ilves: It is a lot easier to change Governments than it is to invade countries. As we saw in 2017—not to get closer to home for you people—if you put your resources across the board into assisting an anti-

NATO, anti-EU presidential candidate, why bother invading? In that sense, it is much cheaper to change Governments through all those means and others.

We have a problem of looking at this in a siloed form—there is cyber, there is disinformation, and there is simply paying people off—as if these were discrete and mutually exclusive activities. From the perpetrator's point of view, these are all different tools that can be used to achieve an end. If you can in fact "disaggregate", to use Donald Rumsfeld's term, either the European Union or NATO, go for it.

Hugh Milward: My fellow panellist's comments are spot on. The direction of travel of technology and the way computing continues to increase, most recently with the move to and the increased use of the cloud, mean that we are increasingly seeing distributed intelligence moving between the cloud and what we call the intelligent edge—embedded information technology devices and sensors. Companies like IDC predict that in just two years from now around 50% of new enterprise IT infrastructure will be at the intelligent edge, rather than in corporate data centres. If you look at the direction of travel of technology, the surface risk also changes. This is why we are talking not just about cyber-threats but about the design and security of technologies like 5G, which connect distributed devices to the intelligent edge.

I have a couple of thoughts there. The rule of law has to be paramount. On the comments about the size and ubiquity of technology companies, it is incredibly important that they operate within the rule of law and that we continue to contribute to the direction of the rule of law.

Secondly, there are definitely ways in which the rule of law can be improved—I think we will get on to that in a minute—including standards, which we have talked about already, and international collaboration on cyber-norms, the malicious use of technology and the way we hold bad actors to account.

Thirdly, we are seeing the number, the level and the intensity of state-sponsored cyber-attacks increasing daily. In many respects, it is not the technologies that are undermining; it is the way that bad actors are using technologies that does the damage, particularly in respect of disinformation and cyber-attacks.

Royston Smith: Does Mr Jaiman want to add anything to that, or shall I move on?

Ashish Jaiman: I just want to add one quick thing—and please call me Ashish. The speed and scale, especially the ubiquitous speed and scale, that most of us have in spreading content across the globe, can very easily be not only weaponised but weaponised at a speed and scale that we have never seen before.

Q20 **Royston Smith:** While I have got you, Ashish, are there any technologies or applications that are currently being overlooked or not being given enough attention by Governments?

Ashish Jaiman: I will put it in the context of the threat models. As Hugh said, the problem is not the technology, but the malicious use of technology. What is overlooked is not the technology itself but the threat models around particular pieces of technology. If we start thinking about technology, which is a great tool to empower but can also be weaponised, we start building threat models. We used to do that in cyber-security, and we have done a pretty good job in building threat models around cyber-security. We should start thinking about building threat models around all the new innovations that we are seeing right now—around AI, 5G and other new technologies like synthetic media. Having that threat model would help us understand the problem better and find effective countermeasures.

Q21 **Royston Smith:** Mr President, you said it is easier to change Governments than it is to invade countries, so you may say that we are overlooking everything, but I was interested in your take on that.

Toomas Ilves: I would add that we have to understand that the old threats have not gone away, but the new threats are no longer kinetic. Everything that we have designed for defence has always been based on kinetic threats. The North Atlantic Treaty Organisation is that not because we are all so wonderful but because of bomber range, fighter plane fuelling, tank logistics and troop movements. But we are living in an era where there is a microsecond difference between attacking a NATO member and attacking Australia or South Korea, so we have to do a lot of rethinking.

The other thing that I was going to mention is that we really have to rise above all these various digital tools. We must not look at them separately. For example, within NATO we have a centre of excellence for cyber-attacks—for cyber. We have a centre of excellence for disinformation, or for strategic communication. We have seen a new phenomenon known as deep fakes. When I turned towards the cyber defence NATO centre, they said, "Oh, that's content. We don't deal with that." When I turned towards the StratCom centre of excellence, they said, "Oh no—that's technical. We don't deal with that," so we have something that is disinformation using AI that falls between the two. What does that mean? Should we build a NATO centre for deep fakes? I don't think so. I think we need to rise above these different silos, look across the silos, and deal with these issues in a more comprehensive and connected way.

Q22 **Royston Smith:** Again because of your opening remarks, are private companies and Governments doing enough to counter technology-enabled disinformation?

Toomas Ilves: No. I wouldn't even say that it is a two-dimensional problem. One is the siloisation problem. The other is, for example, disinformation working hand in hand with cyber-attackers. Take the two best known Russian ones, which the CIA calls APT28 and APT29. In the past seven or eight years, they have attacked the State Department, the US Congress, the Bundestag, German think-tanks, the Dutch Foreign

Ministry, the Italian Foreign Ministry and the Danish Foreign Ministry. They have even attacked WADA, the World Anti-Doping Agency. They of course also probably attacked Macron in 2017.

The information obtained through hacking is then weaponised via the Saint Petersburg troll factory run by Vladimir Putin’s cook, Yevgeny Prigozhin. Not only is it wrong to put these different threats into silos, the other thing that is missing is that there is, at least in the liberal democratic world, no communication between countries. Okay, you have the Five Eyes, but that isn’t enough. A little more than 10 years ago, we discovered a Russian worm in our military network. We went to NATO and said, “Look, we discovered this worm.” The response then—I am told that it would be better now—was, “Oh, you too?” If you think about that, that means that they knew about it but did not tell other members of NATO.

We have silos. Then, in the other direction, we have this understanding of anything related to cyber that probably comes out of the signal intelligence background of what is today called cyber. You have the Five Eyes, but otherwise you do not share that information, and that is clearly dated now.

Q23 **Royston Smith:** Hugh, did you want to add anything to that?

Hugh Milward: I think that is spot on. A lot of work is under way. Companies like ours, Google and others in the private sector are doing a tremendous amount of work in this space, but equally the incredible organisations like the NCSC, the National Crime Agency and others are also doing a lot of work to try to direct this. As the President said, this is always on. It is constant and it has different aspects to it. A cyber-threat in one area will be accompanied by a disinformation threat effectively emanating from the same state-sponsored actor.

The two organisations that we have been tracking recently from Russia are what we call Strontium and Nobelium, but they are known by other names as well—again, deeply active, always on constant attack against the UK’s democratic institutions as much as anything else. We are hampered also by our contractual obligations to our own customers. For example, during covid-19, the NCSC initiated with the Crown Commercial Service an arrangement whereby, if the NHS saw a cyber-threat against one of its trusts, for example, a piece of secondary legislation allowed us to inform the NCSC at the same time that we informed effectively our customer that this is what we were seeing. But it is time limited. It had a sunset clause in it and it ran out halfway through last year. It was rapidly renewed, but it is very restricted to the NHS as well, so we need to start thinking a little more broadly about the obligations on organisations to be able to report the cyber-risks that they face, particularly across the public sector.

Q24 **Royston Smith:** Ashish, can I come to you next? How far do you think the UK Government can go in influencing Russia and other autocracies to behave more responsibly when it comes to using new technologies?

Ashish Jaiman: The most important thing—it was targeted in the first panel—is around attribution. Attribution is an effective tool, so that is one.

The other thing that we should also think about is diplomacy, which you guys know better than us. The last is technology solutions. One thing we should also think about is that at the end of the day these are adversarial tactics. Cyber-security threats are adversarial, and disinformation now is becoming more and more an adversarial tactic very much tied to the cyber-security threat. What nation states should do, especially around coalitions such as NATO, Five Eyes and others is use technology as a counter as well.

Q25 **Royston Smith:** Mr President, before I wrap up and hand back to the Chairman, before I am accused of hogging the whole session, do we currently have enough diplomatic levers, and should Foreign Ministries be thinking about new levers of influence?

Toomas Ilves: We have a fundamental problem with the treaties, which is the approach. We have had two sessions of UNGGE, the UN Group of Governmental Experts, which has tried to deal with these problems. There is an intractable problem between liberal democracies and authoritarian states in that the authoritarian states say, "Sure, we're happy to discuss all these issues of cyber-security and disinformation, but we want to talk about content, and regulate content as well", at which point liberal democracies say, "No, we're not going to engage in discussions of content because freedom of speech is paramount." So that is not working, and on diplomacy, we have seen that it has not done a great job do far. At least I get the impression that at President Biden's meeting two weeks ago there were some implicit threats involved: if you don't stop, we will do it, too. The problem we face among liberal democracies is that we are loth to engage in activities that would disrupt civilian infrastructure, whereas they have had no compunction about it. We could do it just as well. Technologically, it is not a problem to cause disruption. President Biden said, "How would you feel if we disrupted your oil pipelines?", but the west has not done that. Until you can back something up with a genuine—A demonstration of force might be something that perhaps might make them rethink things.

Q26 **Royston Smith:** That is very interesting. Did you want to say something, Hugh?

Hugh Milward: To take that one stage further, in effect, what we are seeing is cyber-attacks on domestic infrastructure in times of peace, where our response is designed for a response in times of war, and we have not yet agreed the norms by which we will respond on something that looks like it is in-between the two.

Royston Smith: Understood. Thank you; thank you, Chairman.

Q27 **Chair:** Before I turn to Bob, can I very quickly pick up on your point there, Hugh? You are speaking, of course, as a private company and not as a state. How do you see yourselves, geographically?

Hugh Milward: I tried to make it clear in my opening remarks that we are big believers in the rule of law. With the UN strategic development goals, for example, each of those goals has one corporate backer behind it. The goal that we back is the one about strong judicial institutions: the rule of law is fundamental, so we are behind the action that liberal democracies can take. That is very clearly where we stand, and we will play a part in moving the agenda forward where we can, in a way that is completely consistent with both the rule of law and protecting the democratic institutions led by like-minded countries.

Q28 **Chair:** It is a challenge, though, for a non-state actor—as a company is, of course—to find where it fits in this challenging environment, because your voice is somewhat different from a state, yet you are often the means of a state action.

Hugh Milward: Yes, and it has been interesting. In slightly more hysterical terms, there has been concern about the power of technology companies to act supranationally, and therefore not falling underneath the rule of law. That is why we have been so insistent on ensuring that we do act within the rule of law, and where we see the necessary requirement for action, we will work to ensure that either the law effectively catches up with the need to act, or that we wait for action until the rule of law is in place.

Chair: Thank you very much. We could go on like this for a while, but I am going to move on, because I know Bob wants to come in, and then Claudia.

Q29 **Bob Seely:** I have two sets of questions. First, to the former President of Estonia, President Ilves, can I ask you this: what was the effect of the 2007 cyber-attack on Estonia? By modern standards, it was relatively unsophisticated and it may not have done permanent damage. What was the reaction at the time, and why didn't that stop Estonia becoming less wired rather than more wired?

Toomas Ilves: First, the immediate response to these attacks was to isolate ourselves. No one could receive anything from a top-layer domain—dot-com, dot-uk, dot-whatever—so at least we were spared. Virtually all digitally based public services using the internet, with the exception of the state-run net, were shut down, as were banks and media. For us, because we had already taken this route, it was not possible to back down, and instead we went in the other direction.

More interesting was the response of, in one case, NATO. Basically, aside from the US and the UK, this was met with this typical "Oh, you're a bunch of east European Russophobes. You are just making this up." The nature of a DDoS—distributed denial of service—attack is that botnets, which are infected computers all over the globe, are directed towards a single server, or another. They said, "I see this comes from Uruguay", or whatever, because they did not understand. A fundamental problem, at least at the time, was the lack of understanding on the part of those dealing with security policy. Basically, you can say that the 2007 attack was the first time cyber fitted a Clausewitzian definition of war as a continuation of policy by other means. For example, it took until 2011 for the first panel on cyber-security to take place; it happened at the Munich security conference—that shows how things have changed. To this day, any book on "cyber-war" begins historically in 2007, because it had never fitted that Clausewitzian definition before.

Q30 **Bob Seely:** In the sense that it was a state attack—so there is no doubt about it, the Russian Federation will obviously deny it, but it was a Russian Federation attack. This fits into a bigger agenda, and we are limiting ourselves, but are you now saying that the concept of war has changed, so it is a contested battle of wills, but not necessarily a violent one?

Toomas Ilves: It can be violent, just not kinetic—it does not fit Newton's second law of force equals mass times acceleration. You don't have mass or acceleration—in fact you don't have time or distance for all intents and purposes on planet Earth. That is what I meant when I said it is no longer kinetic. A cyber-attack on a healthcare system will get people killed.

Q31 **Bob Seely:** But just not by blowing them up?

Toomas Ilves: Right. I will give you an intermediate example. There is a case where a disgruntled employee of the Los Angeles traffic control system turned all LA traffic lights red. Imagine if a state actor turned them all green on a Friday afternoon in Los Angeles. First, a number of people would be killed because ambulances could not get there. It would probably take weeks and weeks to get cars pulled out of there because everyone has gone through a green light. What do you call that? Physically, no one has attacked Los Angeles. On the other hand, you have completely immobilised the city. There are so many variants and this is why we need a more sophisticated concept of what an attack is.

Q32 **Bob Seely:** You mention that you were disappointed by some of the reaction. We could be looking now at warning Russia over Nord Stream 2; warning that if action is taken towards the UK, or the destabilisation of Ukraine, or further cyber-attacks on the west or the Baltic republics, a response will be to slow down and wean ourselves off Russian gas. Is that the sort of thing you were talking about?

Toomas Ilves: Well, Germany would never do that so probably not. You have a most recent case—today, yesterday. Another realm is GPS spoofing which placed your ship in the wrong place, right? All these things are now possible. Again, it can be a casus belli if a ship thinks it is in one place and is in another. These are all possibilities that force us to rethink how we address an attack.

Q33 **Bob Seely:** Turning to Hugh from Microsoft—do you mind if I widen this out a little? There is an issue about the tech giants, and whether they are friends of open and free speech and democracy, or Frankenstein monsters or double-edged swords. The accusation against the major digital players, including Microsoft, although maybe a little bit less so than Google and Facebook, is that you are very good at hoovering up people's personal information but pretty poor at supporting free speech and paying taxes, and that you are now silencing political debate over, for example, the origins of covid, in order to either virtue signal, because corporate—*[Inaudible]*—or because you do not want to upset China. Your commitment to democracy is sometimes a little bit thinner than it might be. Is that fair comment?

Hugh Milward: I do not recognise that description of the way that Microsoft operates, I have to say. We have been, for a long time, supporters of democracy. Perhaps Ashish can illustrate that with some of the works that we have been doing, including looking at the ways in which we shore up democratic institutions that regularly face attack by third parties and the way that we support open journalism, including our backing of, for example, the Australian model for ensuring that small news outlets can continue to thrive in an age where their revenue has been removed. That is in a wide range of different places.

Our social media platform is really pretty limited to the chat function within Xbox Live. Again, that area is moderated. We try to make sure that people abide by our rules of the road, effectively, and are respectful of each other and do not post material that is offensive and so forth, but it is a long way from what you might classify as a social media platform.

Q34 **Bob Seely:** That is understood. It is a fair criticism of me that I am using you to make a wider point about tech giants. Although you do not have very much in the way of social media, you do collect lots of data on people. Do you think, in general, big tech has got that balance right between being responsible over content, ensuring free speech and being responsible corporate citizens—not making vast profits and paying no tax on it, as Microsoft does? To a lot of us, you have not got that balance right. What is really depressing at the moment is that there is a global battle in the 21st century—a soft battle thus far—between new authoritarianism and liberal democracy, and I get the feeling that the big tech companies sometimes forget on which side their bread is buttered.

Hugh Milward: I know you are trying to make a point about global tech companies. I think it is very easy to bundle them all together and call them one thing, but they are really not. They are very different in the way that they operate. They have very different business models. Our business model predominantly does not operate on the basis of customer data. We sell services, and we charge people for those services, such as your Office suite. Predominantly, our revenue comes Azure, which is our cloud.

HMRC is very comfortable with the way in which we pay all the tax that is due. We have been very welcoming of the OECD's principles of changing the way that international tax flows work. We look forward to where that debate will go. I know that you may be referring to some commentary in *The Guardian* recently that referred to the sort of profit that Microsoft seems to have booked in Ireland. I think probably all the tech companies collectively have not made anywhere near that kind of profit in the period that was given. *The Guardian* has now published a retraction of that.

Q35 **Bob Seely:** Was that the story in which they said an Irish subsidiary of Microsoft recorded a profit of £222 billion last year?

Hugh Milward: Yes. Even if you just think about what a profit of £222 billion looks like, it is clearly wrong. They have now published a retraction of that.

Your wider point is about corporate citizenship and whether tech companies are playing the role that they should be playing in this domain. We would say that we are. There is always more that we can do, and we are determined to make sure that we do do more. That is one of the reasons why, for example, we have opened the office, which one of your previous witnesses referenced, in New York. It is in order to make sure that we have engagement with the UN on multilateral discussions around really important things like the way the standards debate globally is going and the way there is a disproportionate level of influence on the direction of travel for standards from different markets and that actually is not favouring the rule of law principle of open democracies. Where we can make a contribution to that, we are determined to make that contribution.

Q36 **Bob Seely:** You're right. I'm just looking at the piece now. The $300 billion was about surplus assets transferred to other companies, in Luxembourg and elsewhere, but you still had an operating profit of $13.6 billion, which is an awful lot of money from one low-tax environment. But let's park that for the moment.

Hugh Milward: I think it's better just to address that, actually. If you take a company and you close that company and transfer its assets to another company, that is booked as a financial transfer. That doesn't mean that it's an operating profit.

Bob Seely: Okay. Let us hope you continue to be as good a corporate partner to various Governments in the west as you say you are. That would be great. Thank you very much indeed.

Chair: Royston, you wanted to come back on this. And then I will come straight to you, Claudia.

Q37 **Royston Smith:** I am sorry, Hugh, that we have to get on to this, but you are here, so it gives us the opportunity. You have said that Microsoft are a big believer in law and order, and I have no reason to doubt that. And Bob Seely talked about tech companies knowing which side their bread is buttered. Can I ask you about LinkedIn, who are owned by Microsoft? It is said that they have contacted some of their users and told them, "Don't use words like 'Tiananmen' and 'Uyghur' in your bios", or they may find themselves blocked in China. How do Microsoft feel about that, and does that sound very much like you are a big believer in law and order? Certainly from a global perspective, we have just done our report on the Xinjiang detention camps and Uyghurs.

Hugh Milward: I'm afraid I'm not familiar with that particular topic; I wasn't aware of that. But it does perhaps illustrate the challenge that organisations face, when they are operating in multi-jurisdictions, as to which set of rules they are going to abide by. A good example of this was a letter that I think all of the tech companies received from the Indian Government asking the tech companies to remove every reference in any publicly available space, including all social media, to the words "Indian variant". So you do have to question at what point you abide by that law—in fact, it wasn't a law; it was merely a request from one politician to the tech companies. But it does become a balancing act; it does become a challenge to be able to make a decision. Generally, we come down on a set of principles. One of those is that we want to look after the interests of our customers, and another is that we want to look after the interests of our employees. If either of those face threats by the organisations or the political environments in which they live, we will try to look out for their interests by offering advice, offering guidance.

I should say that I don't work for LinkedIn. They are owned by Microsoft, but I'm afraid I can't speak for them on this particular issue. If it would help the Committee, I can come back with some specifics about that particular topic[1].

Chair: If you would like to write to us, we would be very grateful.

Royston Smith: Wonderful. Thank you, Chairman. Thank you, Hugh.

Chair: I see that Bob wants to say something. Is it really brief, Bob?

Q38 **Bob Seely:** Yes. It's on what Hugh was just saying. Royston made a great point: this is about changing your behaviour in the west to appease an authoritarian state. I understand absolutely what you say: you need to respect cultural rules, respect laws, etc. But at the same time there is a line. When you are changing your behaviour to people in the west to appease an authoritarian state that has a hugely different approach to law and order from what we do in the west, you are stepping over a line. That is an example, which I am delighted Royston used, of behaviour that is highly questionable and not conducive to supporting a free speech agenda, even if you are respecting other people's differences in law and the fact that China is a one-party state.

Hugh Milward: It is a really great example of how hard it is. Also, we face this very example in the difference between the way the US operates and the way that a number of EU countries operate. The increasing level of Balkanisation of things like the open cloud—the concept of the public cloud—is changing fundamentally, because a number of EU member countries don't have the same level of trust in the activities of the UK Government and the US Government in respect of their data. It is then changing the way in which they respond.

You're absolutely right that different countries have very nuanced views of the way in which some of these quite difficult topics are handled. When it gets on to artificial intelligence, for example, the real challenge there is that we are designing the technology at the same time as we are designing the ethical principles by which we are going to operate that technology. As we do so, we need to be having this kind of dialogue, we need to be listening to the views that you're giving us now, and we need

[1] Microsoft later followed up with a letter to the Committee which can be found here: Correspondence from Microsoft relating to LinkedIn.

to be having the exchange of information, so that we can try to make sure that we are going hand in glove as we go and that those principles by which we operate and we design the future of technology are deeply sensitive to what we need to do and responsive to the societies in which we operate.

Q39 **Claudia Webbe:** These have been deeply fascinating conversations thus far. I am really pleased that our witnesses were able to join us. I just wanted to pick up on that last point, only to say that I think that, globally, we have certain principles that people generally adhere to—things like democracy, fairness, justice and even the right to protest. There are certain things that people take for granted, I guess, to some extent. But when it comes to the tech sector in its most general sense, one sometimes does not know what they stand for. I just wonder, if there is no clarity about what one stands for, whether that can sometimes then consume one when you have got, say, an authoritarian state.

You used the example of India. When civil society in India and globally complained—this won't necessarily apply to you directly at Microsoft, but in terms of Twitter—that India was saying that Twitter should ban users using the words "farmers' protests" and seemingly Twitter complied, that, to me, seems to go beyond what tech giants should be doing or be involved in. I wondered what you might have to say about that, Hugh, and what more we can do to ensure that these lines aren't being crossed, so that we can get to a place where there is this sense of trust, justice, understanding of democracy, and the right to protest, with those protests happening in the field of increasingly new technology.

Hugh Milward: It sounds like you should probably invite some of the other tech companies to answer some of your questions. Twitter would have to answer for the comments you were particularly referring to there.

Again, there isn't really a single view of the tech sector in the way we operate or BT, IBM, Twitter or any number of tech companies operate. In the previous session, Ria made the point that every company is a tech company now.

Q40 **Claudia Webbe:** I am talking about new digital technologies.

Hugh Milward: If you take Azure, which is our cloud offering, we put it there at the service of our customers. Fundamentally, it allows for the smallest company—for an individual, effectively—to use AI in the same way as a multinational can use AI. Fundamentally, it is a powerful democratising force. It puts into the hands of individual start-ups the ability to go to market, to design products and to create new value—even though it is just a start-up or an individual—in the same way that a multinational can.

We can use that fundamental democratising effect of technology and those principles to put technology to service and to address some of society's biggest challenges. That is really what we stand for. It is about saying, "What do we face?" We have just announced that we are the final and 10th sponsor of COP26. We are doing that because we fundamentally believe that technology has a central and core opportunity to address one of the big issues of our time, which is climate change. It is similar with accessibility.

Fundamentally, technology can be put to the service of helping people to engage better with the world around them. That is really what we believe in. I cannot answer for the other technology companies, but it is fundamentally about our core mission, which is to empower every organisation and every person on the planet to achieve more.

Q41 **Claudia Webbe:** President Ilves, to what extent are these new digital technologies reducing the relevance of physical geography to foreign policy and diplomacy, and in what ways?

Toomas Ilves: In the old days, you had the Fulda Gap in NATO, and you worried about the Soviet forces breaking through to the north Atlantic. These days, that is irrelevant. There are other geographies that are of importance, but the point is that you can just as easily attack anyone you want. Instead, we have to rethink what defence we use in that sense.

Personally, I tend to believe that there is an ineluctable splintering of the web between liberal democracies and other countries based on how they treat things, some of which you mentioned. If you have censorship, you are not in the group. If you engage in cyber-attacks, you are not in the group. What will emerge ultimately is a group of countries that respect the rule of law, that prosecute cyber-criminals on their own territory, and that do not engage in disinformation and cyber-attacks. They will have a higher standard of communication among themselves—maybe not quite as high as Five Eyes, but it will none the less allow them to overcome the problem that I mentioned earlier, where they do not communicate that they have been attacked by this group, and some other country has also been attacked by that group, but no one knows.

In the future, the defence of liberal democracies will not be just the north Atlantic but will include Japan, South Korea, Oceania and whatever countries that fit in there. Some minor baby steps have been taken. The NATO centre for cyber-excellence includes not only non-members from Europe—Finland, Sweden and Austria—but, if I am not mistaken, South Korea and Japan, which in one way or another are there as contributory members.

There is also a larger issue, which I would raise, with respect to some of the earlier comments on the transatlantic divide between US-based tech companies and the European/UK response. There are a number of problems in terms of data scraping and use and abuse of personal data. On a higher plane, basically what we have is a race between China and liberal democracies. Russia may be the nuisance country that attacks and does all kinds of damage, but they are really not a player when it comes to technology. Nothing is coming out of Russia and probably nothing will, unless it is stolen.

The problem is, on purely economic competitive terms, the west, defined at least as the transatlantic community, is focused basically on a civil war between Europe and the United States tech companies. While China is making leaps and bounds in progress, Europe with the departure of the UK has ceased to have any role in AI. The third power after the US and China in AI was the UK, so Europe is completely out of it now.

There is a fellow I would recommend to Tom Tugendhat—"fellow" is probably the wrong term. That is Ciaran Martin, who used to be in charge of cyber-security at GCHQ, but is now a professor at Oxford.

Chair: And a good friend of mine.

Toomas Ilves: He had a stunning paper, which I had the honour to listen in on—he gave it to a closed audience at Oxford—on the real security issues facing us. They are not, say, Facebook versus GDPR. They have to do with much broader issues, of which Huawei is an initial case, but which will dominate all kinds of areas as China leaps ahead of everyone, except potentially the United States. Europe and the UK alone will find themselves in the next 10 or 20 years to be dominated by Chinese technology and the economies that go along with that. That was a long answer—sorry.

Q42 **Claudia Webbe:** In your work, you have often argued that the relevance of physical geography to a nation's foreign relations and global influence and security becomes less so, because of the ability for various state actors—civil society organisations and bodies—to be able to connect using technology, which means that territorial boundaries become almost obsolete. People can get involved with knowing what is going on in the way that democracies are operating in, say, global south countries as well as the west, and so on, across a whole variety of spheres, and become quite involved in those operations.

What does that mean for democratic values and institutions? Does this necessitate new methods and channels for Foreign Ministries in promoting and defending them?

Toomas Ilves: An interesting case is Tahrir Square, the 2011 Arab spring events, in which we saw a video taken in Tunisia go viral across the Arab-speaking world. That led to revolutions across the Arab world, including Egypt, Syria, Yemen, Libya and, of course, Tunisia.

Initially, especially on the part of democracy activists, as well as tech companies—Facebook and Twitter, first and foremost—the response was, "Oh, this is great. This is a new development. We can spread democracy through social media with no real financial input. Resourceless civil society can effect change using social media." There is a problem with that. That was 2011. By 2014, Russia had absorbed this lesson and said, "Well, if civil society can do this with no resources, imagine what we can do if we put state resources into these things and weaponise information"—in this case, disinformation.

We saw the first effects in Ukraine, where all kinds of disinformation were spread and easily taken up, initially, by Western news media. We saw it used in the 2015 Dutch referendum on an association agreement for

Ukraine, which was utterly absurd—they used Dutch law in order to get a referendum, then used all kinds of disinformation to get a negative result. Then, once we got to 2016 with the Brexit referendum in the UK and with the US election, then on to the French presidential election in 2017, we saw that civil society had fallen by the wayside. It was a case of massive disinformation with state resources, across the board, from hacking to disinformation and the hybrid use of hacked information in the disinformation.

How much can we spread democracy? It may be that the high point was in 2011 in Tahrir Square, but after that social media has been used more effectively and with huge amounts of resources by authoritarian regimes, which also include Iran and China. China is more involved in tracking its own—not even necessarily citizens—co-ethnics abroad. Iran does a little bit of that, too. In any case, the use of social media now seems to be much more in the hands of state actors than of civil society.

Q43 **Claudia Webbe:** Hugh, Microsoft has been interested in the way in which technology is advancing and in the pace of that. Will you say something about what that means for the way countries can build technology alliances with other countries on matters of technology and responsible behaviour?

Hugh Milward: That is an incredibly important point. I think that technology companies, Governments and civil society have an opportunity to play much better together by supporting those alliances. You can see a number of more formal alliances through the UN or, in fact, the UK's presidency of the G7 was a great opportunity to kickstart a number of different motions in this space. There are also non-governmental alliances: the ITU is a really good example.

To Mr President's point a moment ago—which touched, for example, on the companies that would not necessarily accept an invitation to speak to your Committee, and which we should perhaps be more concerned about than not—is the point about the influence that different bodies have in the decision making of some of the standards bodies, and the way in which we might show up slightly differently and more collaboratively, to ensure that there is a counterbalance to some of the undue influence from certain parts that is detrimental to the way we might want the internet to develop. New IP is one dimension to that.

There are also the more informal alliances, particularly when we are looking at addressing issues around cyber-security more narrowly, where you get motions such as the Christchurch call—I know that was mentioned in the previous session. Also, the Paris call for cyber-security—they are the kind of motions that sound as if they are just words, but fundamentally they drive a direction of travel that creates a sense of momentum that coalesces around a set of ideas, which can more easily be turned into something more tangible.

If there is a start, that is a great start. If the start turns into momentum, that is even better. If that momentum turns into international norms and modes of behaviour, better still.

Q44 **Claudia Webbe:** Thank you for that. I have a few more questions. This centres around the notion of building trust, combatting disinformation and promoting transparency. As private technology companies become increasingly relevant to geopolitics and the shaping of norms and behaviour around technology, how should Foreign Ministries adapt?

Toomas Ilves: In some sense, you have greater outreach possibilities than we ever did. In fact, right now, Estonia is chairing the Security Council this very day at the UN, with the Prime Minister being the Chairman from her office in Tallinn. In that sense, you can do all kinds of things. Another issue is how much influence Estonia has in the P5, which is altogether different.

The disassociation between territory and previous ways of doing things has actually allowed us to do something quite innovative—we offer digital residency, which does not entail political or social rights. In the pre-digital age, the state could identify only those people who live on their territory. If you wanted to set up a business or a bank account in a country, you had to be there. That is no longer true. In the digital era, we can verify your identity, probably better than in the old papers ways. We now have a whole bunch of businesses—70,000 companies have opened up in Estonia since we started the programme. I do not know if I should mention this, but many of them are British companies that want to take advantage of being resident in the European Union, so they can do their business as if they were in the European Union. What is the benefit for us? If you make a profit in the European Union, as a company located in Estonia you pay business taxes in Estonia. But the due diligence requirements are very high. That is one place where geography ceases to play such an important role.

Another thing from a foreign policy-security point of view is that, since we have put all of our critical personal data online and where the integrity is guaranteed by a Blockchain, applying the Vienna Convention on Diplomatic Relations, which covers the extraterritoriality of embassies, we have opened a server in Luxembourg that is a digital embassy; that is, it has extaterritoriality. It has a 24/7 dedicated line of all critical data, meaning healthcare data, property data, court cases, etc. In case we get occupied again, and we have been occupied on average twice a century in the last thousand years—last century was especially bad; we were invaded and occupied seven times. In any case, since this is kind of a recurring tendency for us, in terms of diplomacy and foreign affairs, if we ever get invaded again, we will have a record of everyone who lives and owns property in Estonia, as well as their healthcare data.

This all comes under the rubric of foreign relations, right? I mean, you can do all kinds of creative things if you start thinking about it. If all you have is a hammer, then everything looks like a nail, and if you keep getting invaded you keep looking for ways to save your data in case you are invaded again. So, that's where we are.

Q45 **Claudia Webbe:** Thanks for that. I really want to bring Ashish in on this one—it is in relation to the same question. I mean, we are really talking about the fact that we have had a lot of information that has been accessible to a wide range of people—we have obviously had covid-19; we have had vaccination; we have had global health security; democratic elections; and so on—and there has been the whole issue around trust, in terms of the content, moderation and combating disinformation. What role do Foreign Ministries play in all of this? I ask that because there are examples of increasingly authoritarian Governments that have sought to intervene in certain cases. What are your thoughts on all of that, Ashish?

Ashish Jaiman: One thing that we also have to recognise is that this is a very, very complex problem—disinformation, deep fakes, information operations. It is a complex problem for various reasons. One is the speed and scale that we see now, as well as the fact that there is a conflict between freedom of speech—what you can say—and then how do you figure out even how to define what disinformation is? In simple terms, you can say it is a malicious manipulation of content with a malicious intent; that could be disinformation. But again, proving an intent is super-complex as well, because there is a cultural context and also a lot of nuances there.

So how should we think about it? When we think about it, especially the Foreign Ministry or the external affairs angle to it, can we start thinking about diplomacy? And when we think about diplomacy, we are talking about a couple of things. One is: can we inform and advise the leaders to come up with the right kind of solutions? And when we talk about the right kind of solutions, we actually focus on media literacy as well. Can we not only make consumer-citizens a bit more discerning citizens when they consume information and propagate it, but also the leaders, who are actually making policies and defining knowledge, as well as—sometimes in some jurisdictions—creating new regulations to fight this menace of information operations? So we have to start thinking from that perspective.

The idea that was brought in on the earlier panel was having a technology diplomat—a kind of role in embassies. That role could be super-useful both to channel the technology discussions with the countries or states and to bridge the gap between technology companies, to understand how a multi-stakeholder, multilateral solution, especially around disinformation, can be brought together.

Q46 **Claudia Webbe:** We are talking about the power—and it is power—of private technology, of new digital technology, to influence, because of their growth. Initially, we saw these organisations as tools to enable us to do something different and good, but equally, there is a great deal of distrust. People lack trust in these new industries, new technologies, new digital technologies. Whose tune are they playing and operating to? I want to touch on that a bit further. How can Foreign Ministries help to build trust between citizens and private technology companies, and between Government and those companies?

Hugh, you indicated that Microsoft has a role to play at the forthcoming climate conference, for example, and that could be seen as a force for good in a way. In one respect, there will be those in the global south saying, "Well, to whose tune is Microsoft operating?" Does there need to be a building of trust? If you are weighted towards the benefits of one set of actors, without mitigating or supporting another set, what does that mean in terms of trust in civil society, as opposed to in Governments or in big private companies?

Hugh Milward: That is such an interesting question. Fundamentally, what you are saying is that in the hands of one group of people a particular technology can be a tool, and in the hands of another group of people the same technology can be a weapon. How do you navigate between the two? How do you ensure that you are building trust? Fundamentally, if people do not trust the technology, they will not use it, so inherent in that is the motivation that we have to make sure that people do trust the technology.

Where we net out on this is that, fundamentally, our best interests are in ensuring that we serve society in the best way possible, and that, if we do so successfully, that same society will continue to use our products and services. Our business model is different from others, inasmuch as people vote with their feet. If they decide that they do not want Azure and Office, they will go somewhere else, and we will not collect any revenue. Fundamentally, there is this very close relationship between the service that we offer and the contentment of the customers who use us. At the same time, we recognise very clearly the need to make sure that in everything we do—in all our interactions with our customers and our own people—we are deeply invested in building trust.

Where do we choose to intervene? We should choose to take action where we can do that most effectively, whether that is in ensuring that we are shoring up the fundamental basics of democracy or democratic institutions, applying things like artificial intelligence to drive outcomes that are effectively pro-societal, or making sure we are stepping into difficult debates and are prepared to see them through. That is fundamentally about re-establishing or rebuilding that level of trust between our customers and ourselves. I think that is the direction of travel that all technology companies are going to need to take, because that is effectively what is going to re-establish the trust relationship.

Q47 **Claudia Webbe:** Mr President, do you want to come in? Are you able to touch on how Foreign Ministries can help build trust between citizens and private technology companies, and between Governments and companies?

Toomas Ilves: The first thing that I want to say is that I have to leave at quarter to.

I would not just restrict it to Foreign Ministries, although they too have a role. There is a different way of looking at this. The entire discussion today and generally has focused on the private sector, but there are so many things that could be done outside the private sector. The problem is that, in countries like the UK and the United States, the idea of a secure digital identity is anathema. A secure digital identity is actually one of the three core requirements of successful digitisation. The use by Amazon and other companies of your email address plus a password is utterly ridiculous in this era. The sine qua non—the minimal thing—is two-factor authentication.

There are things that Governments can do, and there is one case of this that exists between Estonia and Finland. Using the system that we have, which is a public-private partnership but is basically national infrastructure, if you are a Finn visiting Estonia or an Estonian visiting Finland and you get sick, you can get a prescription. So, if a Finn comes to Estonia, drinks too much, has too good a time and loses his medicine, he can go to any pharmacy in this different country and, if he can identify himself digitally, he can get his medicine. It is the only place where cross-border services work.

I lived in the centre of Silicon Valley—Palo Alto—for almost four years, and when I wanted to register my child for school, I had to take along a photocopy of my electricity bill, my passport and some strange thing called a DS-2019 form, which certified that I was teaching at Stanford and so forth. I drove to the school headquarters and someone wrote everything out, whereas if I did that in my country, all I would do is log on.

I think that Governments have actually been way, way, way behind, and the private sector has not done a great job. I guess you can commercially get some strong ID, but that still requires the participation of the public sector in order to have any kind of legal validity. What I am saying is that, while we are obsessed with the tech companies, countries have really forgotten the public sector side of services that can be offered, which require genuine security.

At the beginning of the covid outbreak, in the United States, because of the nature of the bureaucracy there, there was a backlog of 3 million passport applications in three months. In Estonia, which of course is smaller, there was no backlog whatever, because if you want a new passport, you do it securely and online, and you don't have to stand in line anywhere.

One thing that you want to look at, especially because it is the one thing that did not fall apart in the 2007 attack on us, is our national system of individuals' private data. That is just something that you should look at.

Q48 **Chair:** May I interrupt? Sorry, Claudia, but we have only a few minutes left and I want to ask a couple of final questions. The way in which Estonia has dealt with this, Mr President, has been very national. How much have you relied on the European Union as a support network, or on your alliance with the United States or NATO? How much have you been able to do genuinely by yourself?

Toomas Ilves: Unfortunately, the rest of the EU are so far behind that it is pointless, frankly, so not much. In fact, it works the other way around. We are trying to push things. One important area where we pushed very hard is the ADOS directive, which means that every country should offer the possibility of a digital identity to its citizens.

Q49 **Chair:** There is a lot of talk at the moment about a third way or maybe even a fourth way, where you have a US standard, a Chinese standard, a European standard or maybe a fourth standard. Do you think that is at all credible?

Toomas Ilves: That is about the only place where the European Union is a power—setting standards, be they phytosanitary or GDPR. It really began with GSM. Others had their own standards, but GSM, which was adopted by the EU, became the worldwide standard for mobile telephony. That is where the EU is a power, and it has such standards. California has basically adopted GDPR but called it the Californian version of it. In that sense, the EU can do things, but it is notoriously sluggish on these matters.

Q50 **Chair:** May I ask one final question, Mr President? How credible is it to be a tech power, as in many ways Estonia is, if you do not have a single digital identity?

Toomas Ilves: You can do a lot of damage, but anyone can do that—the Russians do a lot of damage without any kind of identity system. We should focus on the positive side of things, as services to citizens. We are not much of a power when it comes to damaging others, though we have the brain power to do it if we wanted to do, but we prefer to avoid that realm.

Chair: Excellent. I know you have been extremely generous with your time, so I will draw things to a close. I have to say that one of the things that really struck me about your comments, Mr President, was that they reminded me of the old joke that engineers used to say: "The mechanical engineers make the weapons, and the civil engineers make the targets." Today it sounds like the digital engineers make both. I must say that I am delighted by your comments.

Hugh and Ashish, I am extremely grateful for your insights from a corporate perspective, which is absolutely vital to this inquiry. We have heard some extremely important evidence as to how to begin to think about technology as a foreign policy space and as a space in which we are going to have to act—and in which we do have to act—and about ways in which we should be looking not just at relationships with large companies or technological relationships with countries, but at reaching down below that as to how we ensure that voices that would otherwise not be heard have a say in how standards are set in the changing world that we are facing.

On that note, I thank Mr President, Hugh and Ashish. Thank you very much to my colleagues.