Speech: A free, open, secure cyberspace for all

Introduction

Good morning and thank you, Minister, for your warm introduction.

I am delighted to be in India, and I am grateful to the Observer Research Foundation for this opportunity to address such an esteemed audience.

Before I begin to talk about our shared interests in the future of cyberspace, I'd like to take this opportunity to commend the work of my Indian counterparts.

Minister Prasad, like the UK you face vast and complex domestic, regional and global cyber security challenges and you work tirelessly to keep your citizens and businesses safe.

We both know that the threat of today will be dwarfed by the threat of tomorrow, and so our response too must be ever evolving.

At the same time we both recognise the internet's great potential.

In both of our countries the digital economy forms a significant part of GDP, employs tens of thousands of people and continues to grow quickly.

In India, internet usage is growing at a phenomenal rate every year, and will grow faster still through Prime Minister Modi's exciting vision for a Digital India.

So I turn to one of the most pressing international issues of our time: how to harness the power of the internet while ensuring our safety and security online.

Or to put it another way, how do we collectively continue to build a free, open and secure cyberspace for all?

Evolution of the Internet

I remember hearing about the 'World Wide Web' when I was just completing my law articles in 1990, but could not even begin to imagine the impact it would have.

No recent invention in human history has changed our lives so dramatically or so quickly. This extraordinary creation – the brainchild of a British engineer, Tim Berners Lee – has surely surpassed even his wildest expectations.

An internet worth protecting

Today the internet connects, informs and entertains nearly three billion people across the world. Thanks to mobile phones, we have access to its power virtually anywhere we want.

Never before have ideas, information and products been so universally available.

The internet has transformed vast swathes of the earth from communication black-spots to communication hotspots.

We can access one and a quarter billion websites from our phones, wristwatches, tablets or home computers.

We can control our bank accounts, adjust our heating – or more likely, here in India, your air conditioning – and we can shop for anything from health food to helicopters.

The Challenge

There is no doubt that the internet has spread knowledge and opportunity further and faster than ever before. It has powered extraordinary positive change.

However, the very features of the internet that make it a force for good – its low cost, its global reach and its easy accessibility – also make it attractive to those who wish us harm.

The threat is ever evolving.

From power stations to pace makers; dams to defibrillators; toasters to telecommunication networks, the growth in global connectivity is exposing us all to new risks in ways that could not have been conceived of in a world before the Internet.

We must face the fact that the more we use it and become reliant on it, the greater these risks becomes.

Last year, hackers breached the IT systems of almost half of UK businesses.

In recent months both our National Health Service and our Parliament have suffered cyber attacks.

The Costs of Cyber Crime

It’s easy with cyber security to get lost in the ones and the zeros, but for many in this room, these ones and zeros often come in the form of pounds, dollars and rupees, as they count the cost of cyber attacks.

In fact, cyber attacks have become a global industry in their own right, currently costing the world over $400 billion a year, a figure that is estimated to grow more than fivefold within the next 2 years.

The challenge that faces us all is how to respond to the spectrum of online threats, without restricting the benefits that we know the internet can bring.

It is important to recognise that much of the activity we see online is not actually “new”.

Attempts by rival powers to subvert democratic political processes can be traced back to Persia’s relations with

Athenian Democracy in the 5th and 6th Century BC.

The first documented instance of fraud was in 300BC when a Greek merchant called Hegestratos took out a large insurance policy against his ship and its cargo of corn with the express intention of sinking an empty vessel to defraud his backers.

And it wasn’t long after the advent of the printing press that the medium was being used to produce material that was viewed by the leading powers of the day as dangerous dissent or heresy.

Just as the behaviours we see online are not new, neither do we need to re-invent the solutions. Cyberspace is not a lawless space. Existing criminal and international laws apply online as they do offline, as do fundamental rights and freedoms.

However, while some online activities may be timeless, the scale, speed and anonymity the internet offers are very new indeed and present a uniquely modern challenge.

To address it, we should apply the same qualities that brought us cyberspace itself: energy, creativity and collaboration.

UK Collaborative Approach

This is what is at the heart of the UK approach – working collectively within the international system, with industry and civil society – a multi-stakeholder approach – to address the risks of the digital age while maximising the benefits.

That is why we launched the ‘London Process’ in 2011, to bring people together and further international understanding of how the “rules of the road” for cyberspace might be implemented in practice.

I am delighted that India will be hosting the fifth iteration of the Global Conference on Cyberspace here in Delhi in November.

We take this collaborative approach because the internet is a global resource, which not only stretches across international borders; it also reaches into our offices, our communities and even our children’s bedrooms.

Not only must the governance of the internet be truly global, it must also involve the full range of stakeholders represented here today.

The best analogy I can think of for the UK view of online safety and security is, as a team sport.

A sport where industry, academia, civil society, government, international partners and, above all, the public, play the part of wicketkeeper, slip, gully and deep square leg.

In other words, it is all about working together.

Responding to the cybersecurity challenge

This approach is perhaps seen most clearly in our response to the cybersecurity threat.

With the UK's National Cyber Security Strategy we are seeking to defend our people, businesses and assets across the public and private sectors; to deter and disrupt our adversaries, whether states, criminals or hacktivists; to develop our critical capabilities and to strengthen our cybersecurity sector.

Central to delivery of this Strategy is our National Cyber Security Centre (NCSC), which celebrates its first birthday this week.

Bringing together all of the UK's cyber security expertise into a single body, the NCSC works with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management.

You will hear more about the NCSC's achievements tomorrow, directly from members of the Centre, who have travelled here with me.

Another important part of delivering our strategy is international cooperation.

The UK is working to strengthen partnerships on a bilateral, regional and global level to collectively tackle threats, build confidence and transparency, and strengthen global cybersecurity.

Our partnership with India is a good example.

We have built cooperation at all levels, from heads of government to our excellent working relationship with Dr Rai and relevant parts of the Indian government through interaction between our tech sectors, think-tanks and NGOs. Together we are working to improve cyber security, combat cybercrime, and advance voluntary norms of responsible state behaviour and the application of international law to cyberspace.

We have built cooperation at all levels, from heads of government to our tech sectors and non-governmental organisations.

Terrorist Use of the Internet

This kind of multi-layered approach is vital for strengthening cybersecurity.

The same is true of tackling extremist content online.

This issue is a particular priority for the UK government because the UK is reported to have the biggest online audience in Europe for Jihadist propaganda, and the 5th biggest worldwide after Turkey, the US, Saudi Arabia and Iraq.

We all have a role to play.

First, national governments have a responsibility to provide the legal framework and the resources to stop material being disseminated within our borders. And we must cooperate across borders to stop material that originates overseas.

Secondly, internet service providers have a responsibility to stop terrorist material being uploaded and to take it down more quickly when it is.

Finally, families and community groups have a responsibility to be aware of the dangers and to do what they can to prevent people they know from falling prey to online extremism.

If I may, before I conclude, I would like to set out what action the UK government is taking to tackle this issue of terrorist use of the internet. As I said just now, it is a current priority for us and our Prime Minister Theresa May has been leading global efforts.

She was instrumental in establishing the Global Internet Forum to Counter Terrorism – an industry-led initiative to close down online space for extremist material.

At the UN General Assembly last month, alongside President Macron of France and Prime Minister Gentiloni of Italy, she hosted an event for tech industry leaders and like-minded countries, including India, to find solutions to the threats we face.

She laid down an important challenge to internet service providers: to take down extremist content within two hours of it being posted.

At a national level we are also stepping up our response, using our counter extremism and counter-terrorism strategies to help us remove “safe spaces” for terrorists online.

We are determined to prevent extremists from using cyberspace to sow fear, hatred and division. However, we must also be alert to the fact that they also seek to undermine our values. We must at all costs avoid a response that restricts the very freedoms they seek to undermine, or we will be doing their work for them.

Conclusion

Excellencies, ladies and gentlemen, we must come together in the face of these and other threats.

We must hold fast to the values of decency, fair play and mutual respect.

We must defend the extraordinary opportunities that the internet brings.

Let us come together to keep it free, open and secure in equal measure.

Let us make sure that the internet of tomorrow is a force for good. Thank you.