Speech: Home Secretary speech on cyber security to Commonwealth Business Forum

It’s a great pleasure to be here today with so many representatives from across the Commonwealth and business to celebrate the 25th Commonwealth Heads of Government Summit.

The first ever Commonwealth Heads of Government Meeting was back in 1971 in Singapore.

But 1971 was an important year for another reason too.

That year, computer engineer Ray Tomlinson, working at MIT, sent the first ever email.

Now, this message itself wasn’t particularly earth-shattering, just a series of letters that Tomlinson sent from his computer to the neighbouring one. All the same, it marked a historic moment in the evolution of communication.

Fast forward to now and it is estimated that globally we send a staggering 269 billion emails a day.

The internet is now an integral part of all our lives.

I expect that even since I started talking, some of you have glanced at your phones.

The growth of access to the internet is phenomenal.

It’s estimated that 48% of the population used the internet last year.

71% of the world’s 15 to 24 year olds are now online.

And the internet has revolutionised how we do business too.

Today, a business in India can sell goods to someone in Barbados over the internet and can receive payment in seconds.

A farmer in Kenya can crowdsource a loan from people across continents to pay for new farming equipment.

The internet is now the backbone of our banks, our power grids, our schools, universities and governments.

But we know that while the internet has brought many obvious advantages, it’s also brought new threats.

Threats that continue to grow in scale, sophistication and severity.

And cybercrime costs billions.

In the UK, nearly 7 in 10 large businesses have experienced cybercrime with an average cost of £20,000 per business. Some breaches leave companies on their knees.

And then of course, there's the broader cyber threat.

Hostile state activity in cyberspace is the most alarming expression of that threat.

Over the last year we've seen a significant increase in the scale and severity of malicious cyber activity globally.

We know that there are several established, capable states seeking to exploit computer and communications networks in contravention of their obligations under international law.

Consultations conducted in partnership with the Commonwealth Secretariat and Commonwealth Telecommunications Organisation show that members are concerned about the scale and complexity of cyber attacks from hostile states, groups and individuals who use cyber tools to commit crimes, to project power, to intimidate their adversaries, and to influence and manipulate societies in a manner which makes definitive attribution difficult.

But we have started to call this sort of activity out.

For instance, in 2017, countries across the Commonwealth were hit by the Wannacry ransomware attack, with cases reported in India, Bangladesh, Malaysia, Pakistan, Singapore and Australia among others.

Wannacry was one of the most significant cyber attacks to hit the UK in terms of scale and disruption. It disrupted over a third of NHS Trusts in England and thousands of operations were cancelled, putting lives at risk.

But in partnership with others, we publicly attributed the Wannacry attack to North Korean actors known as the Lazarus Group.

And in February, again in partnership, we called out the Russian military for the destructive NotPetya cyber attack of June 2017.

And on Monday, our National Cyber Security Centre partnered with the US Department for Homeland Security and the FBI and issued, for the first time, a joint technical alert about malicious cyber activity carried out by the Russian government. I know that some Commonwealth partners have supported that statement and it marks an important step in our fight back against state-sponsored aggression in cyberspace.

Together, we need to continue to call out this sort of destructive behaviour.

And when it comes to cyber security, working together really is the best approach.

I know that Australia and New Zealand are doing great work supporting our Pacific Commonwealth Partners with cyber security and that Ghana is sharing expertise with others in Africa. Our very own National Cyber Security Centre and National Crime Agency work globally and with our Commonwealth partners to address cybersecurity and cybercrime.

They've supported the Central Bureau of Investigation of India to provide training on reverse engineering and analysis of malware.

We worked with the Kenyan Police and provided expertise for their first high profile cybercrime investigation which resulted in a successful prosecution.

And we want to continue to build on projects such as the Commonwealth Cyber Crime initiative with Barbados, Botswana and Grenada amongst others. We must continue to work together to address the shared cyber threats and opportunities.

That is why the Commonwealth Cyber Declaration, which foreign ministers and leaders will be considering this week, is such a powerful demonstration of common resolve to address our collective cyber security.

As the world's largest inter-governmental commitment on cyber security co-operation, it sets out our agreed principles and ambitions, and agreement to work more closely together to enhance our collective ability to tackle threats and foster stability in a free, open, inclusive and secure cyberspace.

And earlier today, the UK Prime Minister announced a £5.5 million UK programme supporting cyber security in the Commonwealth to support the implementation the Commonwealth Cyber Declaration by 2020.

This will bring the UK's total programme of support for Commonwealth partners to nearly £15 million over the next 3 years to help improve cyber security capabilities.

So there's important work ahead.

And whether you're here today representing a government, a business or just yourself, one thing should be very clear. And that is that we need to get our cyber security right.

From understanding where the gaps are in our national cyber security, to ensuring that law enforcement agencies have the skills and expertise to investigate cybercrime and provide victims with support. We need to increase public awareness of what good cyber security looks like and what the basic changes – like strong passwords – can make to this.

As today's panellists will I'm sure make clear, cyber security is a shared endeavour. Governments, businesses and individuals must all play their part.

And we also need to ensure that the pipeline of talent going into the technology sector is capable, expert and diverse. As Jeremy Flemming, Head of GCHQ, noted last week, we continue to "need to seek out diversity of talent,

to recruit and retain the best minds”. And we are. We’re throwing our support behind initiatives from the private sector in the UK, like the Tech Talent Charter – a commitment to improve female representation in the tech sector – to demonstrate this.

And I encourage all of you to consider, and share how your businesses and governments are meeting this challenge.

Because diversifying the way we think about security helps combat the diversity of threats.

I want to conclude today by saying this.

Ray Tomlinson was inspired by the promise of the internet to send that first email.

Every day, businesses across the Commonwealth are growing and thriving because of it.

And while there are threats that we all now recognise, I believe that by working together we can make sure that the promise of the internet is realised while the threats are combated.

Thank you.