Speech: Addressing the Global Cyber Challenge

I am delighted to be here with you today.

We meet at an auspicious time.

A time of change faster than anyone has known. Around the world, we are living through a technological revolution which brings unimaginable opportunity. And with this unimaginable opportunity, so too risks unknown just a few short years ago.

The internet fifty years ago. The world wide web, twenty five years after that. Ten years ago, social media and the smartphone, and now artificial intelligence and machine learning. New generic technologies that have sporned a thousand revolutions, from fintech, to lawtech, to edtech or govtech, indeed in almost every area of our lives. The pace of change is relentless. And if you don't much like change, I've got bad news. For the nature of artificial intelligence means we are likely to be experiencing, right now, the slowest change we will see for the rest of our lifetimes.

So now is a good moment to bring together some of the leading nations in the world of digital technology. And it's good to be here in Singapore for this discussion. Like us, Singapore is a small island nation with an emphatically global reach, that revels in a culture that's open and looks for trading partners the world over among freinds and neighbours, near and far.

And amongst friends, let us be open and talk not just of those opportunities, but how we protect those opportunities, for the good of all our citizens, from those who would do harm.

Since its conception, the internet has brought enormous freedom. But the internet is growing up. To protect that freedom as it grows we must also be restless in protecting a safety and security online.

From the pioneering work of Ada Lovelace and Charles Babbage to the visionary Tim Berners-Lee, the UK has always been at the forefront of digital innovation.

Yet around the world, none of us can rest on our laurels. For each nation, even areas where our strengths are well-established, such as our world-renowned creative industries, are being transformed, and kept at the cutting edge, by developments in technology.

I feel this keenly, as before I became the Digital Minister, my first job was solving the Y2K bug in cobol. Thankfully, that went ok.

Yet even the most enthusiastic supporter of new technology must acknowledge that it also brings risks. The challenge we now face is how to harness the power of emerging technology so it works always in our favour, always to

improve the quality of people's lives, and that where it poses dangers we mitigate against them.

In 2011 we hosted the London Conference on Cyberspace, a discussion that continues in New Delhi later this year. From ASEAN to the UN, Interpol to ICANN, we are strengthening our partnerships on a bilateral, regional and global level to collectively tackle threats, build confidence and transparency, and strengthen global cyber security.

That includes building capacity in less developed nations so they can combat threats at source. This work involves supporting the development and implementation of national cyber security strategies, and we've supported capacity building projects in over 50 countries in the past few years.

As we negotiate our exit from the European Union, and position ourselves as Global Britain, we aim to be even more open to collaboration, with all our international friends and partners. In this age of digital we are all becoming more and more connected. It is estimated that in less than a decade the Internet will connect one trillion things.

Both our countries will take on major responsibilities next year. Singapore will be chair of ASEAN and the United Kingdom will host the Commonwealth Summit in London. I am sure these will both be great opportunities to deepen our friendship and strengthen our working relationships.

Today I'd like to share with you the principles we apply to the cyber challenge:

Principles of openness to new ideas, of adaption to change; and preparing for the future.

How we seek to seize the opportunities of the growing tech industry, how we adapt to the changing environment, and how we are preparing for what lies ahead.

The first principle is to be open and optimistic about the opportunities digital technology is creating, for businesses and for all citizens. We seek an internet that is open and free. And we seek a tech industry that is vibrant and innovative. The UK's tech industry has huge momentum, is growing strongly, and is ripe for investment.

Since 2001, tech industries have created 3.5 million new jobs in the UK, more than four times the number that have been replaced. London is now recognised as one of the top tech clusters in the world, and we have internationally competitive hubs across the whole UK. Over just the last year a whole series of multi-billion pound investments have been agreed.

This openness and this technology is helping our citizens, to learn, to better manage their finances, to access government services and simply be better connected to their friends, their family and to new acquaintances. In short, technology improves people's lives.

So our first principle is never to see just the threat, but keep front of

mind the fundamental openness of the internet, and its power to do good.

The second principle is to be ready to respond to change and honest about the risks.

The UK categorises cyber crime as a tier one threat to our national security. Since 2011 we have had in place a National Cyber Security Strategy, which sets out how a full spectrum plan.

The Strategy covers the direct tasks we in Government must take to detect threats, deter and disrupt adversaries, and keep Britain secure online. But moreover, it recognises that we can't do this alone.

Our full spectrum approach ranges from developing the new skills and expertise we need, supporting the cyber ecosystem, collaboration with critical infrastructure, the established cyber industry, start ups, and academia to protect our national security and protect the public's way of life, while contrinuting to our prosperity and building a more trusted and resilient digital environment. I've been struck here in Singapore just how similar the challenges, and the responses are.

Our growing expertise was perhaps best showcased during the 2012 Olympics. The London games were the first ever "digital games" – the first to provide public Wi-Fi access in all Olympic venues, with more content broadcast online than ever before, and much of it accessed via mobile devices – and yet, despite a peak of over 11,000 attacks per second, the network was never once compromised.

We are now six years into that Strategy. In the time since, our cyber security industry has gone from strength to strength. The workforce has grown by 160 per cent and cyber security exports were worth £1.5 billion to the UK last year alone. I'm delighted that many of our leading cyber security businesses are here this week too.

UK universities play a critical role at the forefront of research into cyber security. Because while we address the challenges of today we must work to anticipate those of tomorrow. We have awarded fourteen UK Universities the status of Academic Centre of Excellence in Cyber Security Research, reflecting world class research.

Last year, we refreshed the Strategy. The refresh had at its heart one inescapable fact we had learned: that successful cyber defence requires the collaboration of government, academia, and business. A strong cyber ecosystem needs all three.

Based on that insight, we put together and opened our new National Cyber Security Centre as the authoritative voice on cyber in the UK. As we designed it, we looked around the world to see best practice, including at your CSA here.

The NCSC is formally part of GCHQ, but culturally reaches outside the secure fence to draw on academia, and work with and inform businesses, citizens and the public sector about emerging threats, to provide very practical support

when attacks happen, talk to the public, work with international partners, and educate our nation on how best to stay safe online. Crucially, it brings together national leadership on cyber security in one place.

Our safety, of course, means our friends' and partners' safety, whenever you do business with us. We are committed to making the UK the most secure place in the world for digital and online activity. Respected, and most importantly, trusted.

So this is how we are adapting to the constantly changing risks.

Our third principle, is always to look to the future.

For we much cite cyber security within a bigger attitude we take to how digital technology is transforming society's norms.

Digital technology is a force for good in the world. To keep it that way, we are proposing a new framework, a new global consensus, for how we interact, do business and participate online.

The aim is to protect and promote freedom online, by ensuring that we promote liberal values that underpin freedom while preventing harm online. Our starting point is that the boundaries and norms that exist off-line also apply in the online world.

This approach lies at the heart of our proposed Digital Charter, recently announced by Her Majesty the Queen. The Charter seeks to balance freedom and responsibility online while establishing a new framework for how we all conduct our digital business.

Every society is facing the same sorts of challenges. And by the nature of the technology many of the solutions are global too. Local nuances will depend on each country's culture, but ultimately this balance is needed everywhere.

So our hope, if we get all this right, other countries will want to join us.

Humanity, the world over, we share this technology. Together we have developed it, and together people worldwide now collaborate to develop it further.

We are all connected by it, and harmony will lie in – perhaps even depend upon – a shared sense of its norms. The debate is moving quickly, as the pace of technology increases. As more and more of how we interact – our society, in short – moves online we must be sure it abides by the rules of decency, fair play, and mutual respect we have all built in the offline world.

Cyber security sits in this context.

So let us be clear. We are part of something much bigger than ourselves. We have a job to do.

So let us keep talking, let us keep sharing, so we reach a mutual

understanding of how we can best harness this amazing new technology, for the benefit of all mankind.