Minister for Digital speech at SINET Global Cybersecurity Innovation Summit

Good afternoon.

Thank you to SINET for organising this event and thank you to all attendees, especially those colleagues who have travelled from the US.

SINET plays an important role in connecting the global cyber ecosystem of innovators, investors and customers – be it private or public sectors.

It's great to have you back here for a sixth year and I hope we'll see you again next year.

It's an exciting period, not just for SINET, but for us as a nation. This is a pro-technology Government and I think we need to re-emphasise that, because while regulation is hugely important, the benefits of technology cannot be overstated and in DCMS we're trying to drive forward an exciting digital agenda.

We're improving digital infrastructure, by aiming for nationwide connectivity and we're tackling the issues generated by the digital agenda, for example through our work on data ethics and online harms.

And we're supporting AI and 5G, so that the nation – wherever you are in the country – can benefit from that technology..

Underpinning all of this is our strong and growing cyber security sector. It is one of the strengths we can use as we build our new role in the world.

So today in this short speech I'd like to give you three quick things:

First is to launch our latest UK cyber sectoral analysis report – some copies of which are in the room, and I'd like to take this opportunity to outline some thoughts on the current state of play of the sector;

Second – to look at what my department, is doing across cyber security;

And third, to look to the future at that strategy.

Firstly, we've been delivering our National Cyber Security Strategy for four years now. And we have made some really great progress.

With £1.9 billion invested to protect the nation online, which has greatly increased our defences, building on the 2016 launch of the National Cyber Security Centre.

Programmes like Active Cyber Defence, which is helping defend the UK at a national level dovetails with a host of other more consumer-focused things that look at everything from phishing emails to malicious websites.

Protecting the UK at every level has to be a top priority for the Government. And that means:

Seeking to reducing the threat from those seeking to harm the UK's interests;

Promoting a trusted and secure digital environment;

And continuing to build cyber resilience across Government, our economy and society.

That nexus is how we will tackle some of the problems that I think everyone here will agree we face.

There's a crucial foundation for meeting these aims and that's a strong, homegrown cyber security industry.

So today we see new figures from our cyber sectoral analysis – which tells a hugely positive story about our cyber security sector.

Since 2017, we have seen a 44% growth in the number of cyber security firms in the UK up to over 1,200 at the end of 2019.

This growth is the equivalent to a new cyber security business being registered in the UK every week.

There are now approximately 43,000 Full Time employees which is up more than a third since 2017.

And, the sector's Gross Value Added (GVA) is over £3.7bn – that's up 60% in just the last two years.

And that growth has been driven by several factors:

The widely acknowledged world-leading technological capability that's here already in the UK,

There's also significant support from industry – from the public and private sectors,

And there's sustainable, predictable, sensible, regulation, primarily in the form of GDPR and finally, investment.

2019 was a record year for cyber security investment, with almost £350m in fundraising across eighty deals. And, indeed, over the past four years total investment in the UK cyber security sector has comfortably passed the £1 billion mark.

They're just some of the highlights of the report, which also outlines the growing diversification of the UK cyber sector, with the growth of emerging sub-sectors such as Internet of Things security, and post-quantum cryptography.

There's a lot in there – I'd encourage you to pick up a copy.

But we won’t rest on our laurels. To remain as one of the world-leaders, there’s more work to do.

We, as Government, will continue to support the sector. We must ensure the most ground-breaking products and services, which offer the potential to keep us ahead of the cyber threat, make it into the market.

This includes ensuring viable early-stage companies are able to secure the investment they need for developing, testing and expanding their offer. And I know so much of that is what SINET is all about today.

We will continue our journey to improve how Government buys cyber security products and services – through initiatives such as the not terribly snappily-named Cyber Security Services Dynamic Purchasing System – never was there a less dynamic name. This aims to give the SME market increased opportunities to bid for Government cyber security contracts.

So when we talk about one cyber business a week being created, it’s that sort of thing that allows these small businesses to prosper and to thrive

And last – but by no means least – we have an eye on regional disparity. This Government and the Prime Minister has a ‘levelling up agenda’ to ensure no region of the UK is left behind. And at the moment, we’re very conscious that talent may be evenly spread across the country – but opportunity is not.

Today’s statistics show almost three quarters of the UK’s cyber security workforce is in London and the South East. We need to ensure all our programmes and initiatives are truly national – reaching all parts of the country.

Which leads me to talk about what we are currently doing when it comes to growth and innovation.

We’ve got world-class universities, ground-breaking research and an environment which makes the UK one of the easiest places to start a business, we have some of the most innovative cyber security companies in the world.

But we need more of them to help us meet future challenges. So we have launched a number of targeted initiatives to incubate and accelerate, and support people since 2016.

Hopefully, some of these names will be familiar to this audience:: the Cyber Academic Start-Up Programme (Cyber ASAP), HutZero, Cyber101, and the NCSC Cyber Accelerator. Or taking one specific example – LORCA. the London Cyber Innovation Centre -has just taken on its fourth cohort with 20 cyber startups joining the programme.

This is the largest cohort to date and it demonstrates the strength and attractiveness of the UK market. 35 cyber startups have participated in LORCA’s first three cohorts, and they have gone on to raise over £60million since joining the programme. It’s a really good example of how Government can work with industry to make sure that companies thrive.

We are also working hard to protect the public and industry. Earlier this week we published the Government's response to the consultation on improving the security of the Internet of Things (IoT).

It's an area where decisive action has been widely welcomed by industry but also where action is clearly needed. Citizens' privacy and safety can't be put at risk because security is not built into consumer IoT products from the ground up. We will make sure this is the case.

It's a staged approach starting with a Code of Practice for Consumer IoT Security, but it's by no means the end. This is a starting point and our work on this will continue.

We have also decided to expand the secure by design project to incorporate improving the cyber security of routers, apps and the use of consumer IoT devices within enterprises.

That sits alongside efforts within the European Telecommunications Standards Institute to transpose technical specifications and is another example of the UK working with bodies around the world to offer coherent regulation to the whole sector.

These three areas have been selected because they are part of the supporting infrastructure associated with consumer IoT devices and they will support future efforts and we'll look to expand that relatively quickly.

You may also be aware my department is currently undertaking a Review of Cyber Security Incentives and Regulations. The Review is looking at what more Government can do to incentivise good cyber risk management across the economy, because we recognise that prevention has to be better than cure.

We've been working closely with industry to understand the barriers and the effectiveness of existing regulation and identify where more action is possible and needed.

And we're going to publish an update on this pretty soon, with the call for views closing last month.

You will get the sense there's real activity going on in the area. Not just where the sector acknowledges that regulation is needed but where there's also a real public demand in a way that wasn't the case just a short time ago.

To support all this work, it is important we continue to improve skills at every level – not just in schools and people coming out of universities, but in the whole workplace.

Today's report shows three in five cyber security businesses are struggling to find the skilled people they need. We need to address this to ensure we continue the pace of growth in the sector. Because without providing that pipeline this will simply not be sustainable.

So building a cyber security workforce fit for the future is far more complex

than simply training more cyber security professionals. It is about ensuring the UK has the right level and blend of cyber security capability.

Through CyberFirst and CyberDiscovery, we're developing the professionals of the future. I want to effect longer term change to statutory education to ensure citizens have the digital/cyber skills and opportunities necessary to participate in the economy, right from the very beginning

In the immediate term, the government will continue to develop extra-curricular cyber security inspiration and learning opportunities. The CyberFirst programme has already engaged over 50,000 young people to consider cyber security and computing careers.

We are also setting up the UK Cyber Security Council by March next year. This is a world first: setting up an independent entity to bring coherence and structure to the complex professional cyber security landscape – that is built fundamentally on the idea that Government can be a great convener, but we don't have the monopoly on good ideas in the sector.

The council will make it easier for individuals to pursue and develop a career in cyber security both now and in the future.

And alongside NCSC I recently attended the launch of our new Cyber Security Body of Knowledge ("CyBOK"). This is a new, open source reference tool which sets out the foundation knowledge areas which make up the discipline of cyber security. CYBOK provides the basic definitions that allow Britain to take a foundational role in this sector, but also it will allow Britain to play its part on the world stage. This is why it's so important to work alongside GCHQ and NCSC to provide an open document which will allow the sector to move forwards.

I hope this has been a helpful update on what the Government's doing and our commitment to cyber security. It is multifaceted but i hope you also get the sense that it is going one coherent and confidently pro-technology direction.

We are now looking to the future and developing our thinking for what happens beyond 2021. I would like to thank you for all of your work so far, and all of your collaboration. It's collaboration that will be key to this area.

May we continue to work together in our ambition to make the UK the safest place to be online.

Thank you.