Chancellor of the Duchy of Lancaster speech at Cyber UK

Thank you, Lindy. Good morning colleagues.

Across the Cabinet Office and No10 we see the range of threats that our country faces.

Core to our defence is the work of you Lindy, and your colleagues at the National Cyber Security Centre. So firstly a huge thank you to you, but also to all those in the room who do so much to keep us safe.

And it is these threats that I want to talk about this morning – particularly in the context of Russia's brutal invasion of Ukraine.

But also the huge opportunity that cyber in the UK currently presents, including setting out the whole of society approach that is integral to tackling those threats but also achieving the UK's potential and indeed building on the comments of Sir Jeremy yesterday.

Much progress to protect us from the risk of internet-based attacks has been made since the launch of the UK's first National Cyber Strategy, with cyber experts thwarting 2.7 million online scams last year alone – more than four times that of 2020.

The NCSC has said that it believes that Russia continues to pose a significant and enduring cyber threat to the UK.

And yesterday, the UK – along with the EU, the US and other allies – said that Russia was responsible for a series of cyberattacks mounted since the invasion of Ukraine.

Their impact has been felt across Europe, in disrupted access to online services and even in the operation of wind farms.

And Russia has said it sees the UK's support for Ukraine as 'unprecedented hostile actions' – and as Avril Haines said yesterday, Putin is preparing for a long conflict.

So we must all, therefore, consider the likely long-term threat, so that we are as prepared as we possibly can be.

And the greatest cyber threat to the UK – one now deemed severe enough to pose a national security threat – is from ransomware attacks.

Should the UK face an attack on the scale previously inflicted on Ukraine's critical national infrastructure sites, businesses and the public should not expect to receive advance warning.

Preparedness is therefore essential.

And our defences must be in place: ready for whatever comes in whatever way.

This is why the work, Lindy, of the NCSC is so important.

And I am sure many of you here today have had the benefit of their knowledge and free resources.

But it is crucial that we spread the word wider.

I was delighted to learn that the NCSC's cyber advice for businesses was accessed over 100,000 times after Tony Danker, the director general of the CBI, and I wrote a piece for The Times.

And that 3,000 schools have accessed the NCSC's new cyber defence tools for schools in the first week after its release.

But of course there is no room for complacency.

Every member of the public has their part to play; every company in a supply chain can make sure they are not the weakest link.

Because making sure we are ready, as Sir Jeremy said yesterday, is a whole of society effort.

And that is one reason why the conference CyberUK is a calendar highlight – an opportunity to channel the expertise, enthusiasm and enterprise across government and business.

But also a great opportunity to shine a light on the national success story that digital and cyber has become.

Thanks to our work together, I am determined that the UK will be the world leader for innovation, gaining a digital education, and indeed having an open, safe and reliable internet.

And this allows us to take full advantage of the broader social and economic opportunities of the digital age, which is at the core of our National Cyber Strategy.

And make no mistake: the record £2.6 billion of Government funding is a statement of our intent.

As the Prime Minister has said: 'We want the UK to regain its status as a science superpower, and in doing so to level up.'

Cyber is key to this mission.

It is no accident that we are here today in the heart of Cyber Wales's Ecosystem.

Having previously met in Glasgow.

And next year we will be off to Belfast.

Evidence of the Union working to benefit the whole of the United Kingdom.

I also note, as many in the room will be aware, that today is the 25th anniversary of the supercomputer Deep Blue beating the chess champion Garry Kasparov – in a man versus machine contest that indeed astonished the world.

Now back then, Deep Blue was a project costing $100million. The computer weighed 1.4 tons with two, six-foot five-inch black towers.

Compare that today, to the mobile phones in our pockets matching it for processing power.

Such is the speed of progress, digital technology has already grown to touch every aspect of our lives.

Democratising threats, but also playing an important part in our future growth, with the potential for huge economic gains.

Look at what the cyber security sector alone contributed to the UK economy last year: generating £10.1 billion in revenue and it attracted more than a billion pounds in investment.

Thanks to 6,000 new jobs being created, over 52,000 people are now employed in cyber security and – I think importantly – more than half of them are outside London and the South East.

So as well as Wales, cyber security clusters are flourishing in Scotland, Northern Ireland, in the North West and in the East Midlands.

But we want to see more start-ups – like the new collaboration between NCSC and the five tech companies to develop low-cost ways to tackle ransomware attacks which is testimony to the UK being the best place for innovation outside Silicon Valley.

As the country builds back from the pandemic, the cyber skills revolution will help fuel growth, equip people to build and switch into new careers.

And to stay working where they grew up, spreading opportunity all around the UK.

Through our CyberFirst bursary programme, more than 100 students receive £4,000 and eight weeks paid training or development work with government and industry; leading to a full-time role when they graduate.

And now those working in cyber– including indeed people here today – will have the chance to become chartered professionals, as the UK Cyber Security Council has been granted its Royal Charter in recognition of the invaluable work it is doing to raise standards and ensure good career pathways.

Of course, investment in business and skills is immensely important to the economy and jobs. But it is also essential to help us preserve the UK’s core values of democracy and free speech – as we are doing through our Online Harms Bill.

From my conversations with heads of schools, business leaders and chief executives, the message of the need to keep people safe online is indeed landing and it's spreading; with key sectors stepping up to do their bit.

In schools, we now have more than 1,500 teachers signed up to deliver our Cyber Explorers programme, seeding their enthusiasm in younger students for maintaining a safe and resilient cyber space: and I'm indeed looking forward to meeting pupils from St Joseph's School here in Newport to hear their experiences of the CyberFirst Girls Competition.

We also have the National Cyber Force combining the hard and soft power from our military and intelligence services to counter the threats that we face.

And Government has been working with partners across the sector on legislation in order to help keep us safe online.

We're protecting consumers by enforcing minimum standards in connected products, through the Product Security and Telecommunications Infrastructure Bill – so the 'Internet of Things' doesn't become the 'Internet of Threats'.

Telecoms operators that fail to meet security standards will face heavier Ofcom fines under the Telecommunications Security Act.

And just yesterday the Data Reform Bill, in the Queen's Speech will ensure that personal data is protected to a higher standard, and enable stronger action against organisations for a breach.

Together this legislation will play a significant role, but we also alongside it require a global approach.

In these uncertain times, international allies are essential: in intelligence-sharing, shaping the governance of cyberspace, and deterring irresponsible behaviour and ensuring cyberspace remains free, open, peaceful and secure.

The road to free and resilient cyberspace runs through our friends in Warsaw and Bucharest all the way to Kyiv.

And the UK was among the first states to set out how the rules-based international order extends to cyberspace – and it's something my colleague Suella Braverman, the Attorney General, will be saying more about at Chatham House next week.

Last year, when I launched the National Cyber Strategy, we said that Ransomware had become the most significant cyber threat facing the UK. It is therefore imperative that we continue to prepare for the future, and learn from past attacks – at home and indeed abroad.

We must not drop our guard, underestimate the threat or take our eye off the ball when it comes to our cyber defences across society.

In the run-up to the Ukraine invasion, Russia unleashed deliberate and malicious attacks against Ukraine.

The Ukrainian financial sector was targeted by distributed denial of service attacks that took websites offline.

With the UK government declaring the Russian Main Intelligence Directorate, the GRU, as being involved.

Since then, evolving intelligence about Moscow exploring options for cyberattacks prompted last month's joint advisory from the UK and our Five Eyes allies – that Russia's invasion of Ukraine could expose organisations within and beyond the region to increased malicious cyber activity.

Some UK citizens have already felt the impact of cyberattacks.

And some authorities estimate that in 2020, ransomware attacks may have cost the UK economy a minimum of £615 million.

Over the past year, the National Crime Agency has received on average one report from victims of a Russia-based group responsible for ransomware attacks in the week. One report a week. Indeed, some authorities have estimated that over the last year global ransomware payments are up 144%, and the average demand is $2.2 million.

But the number of incidents – and indeed their economic cost to the UK – is likely to be much higher. Law enforcement teams believe that most attacks go unreported: perhaps through embarrassment or a reluctance to admit that money has indeed changed hands.

So, I would encourage any organisation that suffers an attack to come forward, report it to Action Fraud who run our 24/7 cyber reporting line.

By doing so, you will help us to strengthen our individual and collective resilience as we learn from each other.

In one attack in the UK, the National Crime Agency alerted a public sector organisation to an ongoing breach of its systems. Within hours, the NCA had identified the compromised services and located the exfiltrated data, which it later managed to take down; so that no personal information got out.

What we learned is that our controls quickly spotted the incident and our reaction was swift.

And we were then able to share useful evidence with industries so they can learn and prepare for similar attacks.

The government is stress-testing its own defences, too.

The more complete our security picture, the better we would handle any attack.

And in the context of our most capable adversaries becoming more sophisticated, I can announce that we have agreed support for the next decade of UK cryptographic capabilities – nothing less than the entire ecosystem that keeps government safe – recognising the vital national importance of our

sensitive sovereign Crypt-Key technology.

Now, computer professionals tell me there is only one sure-fire way to know a computer is never hacked. Never connect it to the internet.

But – let's be realistic. That's not an option.

Which is why we have to work together.

Through the NCSC's world-leading tools and advice.

Through acting with international allies.

Through legislation.

Through protecting our own government systems.

But most importantly through harnessing our collective strengths and acting as one, building, as Sir Jeremy set out yesterday, a whole of society response.

This is at the heart of the National Cyber Strategy, treating the cyber domain as no longer being a niche concern simply for the IT team – but as a wide-ranging grand initiative.

Being a responsible, durable, effective cyber power cannot be achieved by government alone.

So we want to work with industry, universities, schools and individual citizens getting involved.

Working together. As a whole society.

Thank you very much.