Home Secretary Priti Patel speech to CyberUK Conference

Good afternoon,

Let me start by thanking Lindy and the whole National Cyber Security Centre team for inviting me to join you today.

Today we are discussing many of the most challenging and important issues we face as a country. In light of the seriousness of these topics it is a privilege for me, as Home Secretary, to outline my priorities and observations on cyber security with you.

The efforts of the NCSC and the work you all do to protect our country in cyberspace are simply outstanding.

These efforts may not always be front page news, but in my role I know what you do here is at the forefront of defending our nation and keeping our people safe.

British businesses and the public are safer because of these efforts and the way in which you work to bring together intelligence and technology to protect people and our institutions.

Cyber continues to revolutionise the way we all live.

The last year has brought that home more than ever before.

Online communications, traffic and the volume that we see on online platform continues to grow.

And that impacts how we guard our own national security and brings new challenges while highlighting new threats, often exposing many new gaps that we have to close.

Cyber is now a core component of our homeland security mission, with effective cyber defences critical to making the UK a responsible Cyber Power, as set out in our recently published Integrated Review.

We are taking a new, comprehensive approach to strengthen our position as a democratic cyber power.

Protecting and promoting our interests in cyberspace, while also detecting, disrupting and deterring our adversaries.

While continuing to shape, influence and unlock tomorrow’s technologies and opportunities so they are safe, secure and open.

We want to make the United Kingdom, and the lives and livelihoods of our people, stronger and more resilient to the threats we face and ready for the

opportunities ahead.

As Home Secretary, it is my responsibility and duty to keep our citizens safe and the country secure, while protecting economic prosperity.

Cyber security and resilience are increasingly important and integral parts of my job. This includes our domestic response to all kinds of cyber threats, whether they be from states with hostile intent, organised criminals, terrorists, or from elsewhere.

Throughout the last year, we responded to new threats, including working with the pharmaceutical industry and the NHS to help protect them from the cyber threats they faced while working to develop vaccines to beat COVID-19.

As all of you in this audience will be aware, the threats facing the UK in the cyberspace – to our citizens, our businesses, academia and to the government – are real and significant.

The picture is diverse, spanning state and state-sponsored actors, organised crime groups, and criminals seeking to profit by defrauding citizens and businesses online.

The scale of this type of criminality is truly shocking. In the year ending September 2020, there were an estimated 1.7 million cyber dependent crimes experienced by adults in England and Wales.

The overall cost of computer misuse incidents against individuals, including hacking into personal computers and email accounts and stealing of personal data and imagery, has been estimated at over £1 billion.

And nearly 2 out of every 5 businesses in the UK identified at least one cyber security breach or attack in the last 12 months.

These are not just statistics. The impact of these breaches and attacks have a profound and lasting impact on people and their lives and livelihoods.

These crimes are not victimless. They cause real harm to people and businesses.

One of the biggest challenges we face in tackling these threats is the breadth of ways in which they can manifest themselves, often causing both financial suffering and long term damage.

The use of networked cameras to spy on and harass individuals…

The operation of criminal websites that sell compromised details, fuelling further cyber crimes and fraud…

The attack by criminals on services essential to the economy, such as the attack on fuel pipelines in the US last week…

And as you will have heard earlier from the CEO of Solar Winds, cyber operations are often highly sophisticated, and many are very likely to be

state sponsored.

The hack on Solar Winds has shown that state actors have significant capability. We need to be able to understand that threat, protect ourselves from it, and bolster our cyber resilience.

While addressing the danger from state and state-sponsored actors, it is rightly a key priority.

We also know that criminal groups have the intent and technical means to operate in cyber space.

The NCSC Annual Report sets out that ransomware incidents handled by the Centre have been increasing.

Cyber criminals have increasingly focused on companies and organisations. Taking the time to research their target so they can maximise their chances of releasing higher sums of money through extortion.

In the face of such complex and often inter-linked threats, it is crucial that we join ourselves up, and have a clear and effective response so that our citizens and businesses are safe and can operate safely and securely online.

Government has a strong position against paying ransoms to criminals, including when targeted by ransomware. Paying a ransom in response to ransomware does not guarantee a successful outcome.

It will not protect networks from future attacks, nor will it prevent the possibility of future data leaks. In fact, paying a ransom is likely to encourage criminals to continue to use this approach.

There is action that organisations can take.

Be as prepared and engage with the NCSC and law enforcement as soon as you can, so they can assist with understanding and mitigating the incident.

Understand the consequences of an incident and how it will affect your organisation in the future. This is not just about loss of data; there can be real disruption and significant impacts.

Learn from incidents – prepare and exercise your response.

Ransomware, like other cybercrime types, has no boundaries. The challenge of investigating and identifying those responsible is one we share with our international partners.

Recently, Five Eyes interior ministers have agreed to work together to prevent, discourage and counter the threat of ransomware.

The threats we face are significant and evolving. But just as our adversaries are continually developing their tactics, we are always seeking new ways to bolster our defences.

And we are making progress. Funding from the National Cyber Security Programme has completely transformed our capability – from improving the response of local police forces through bringing the most sophisticated organised crime groups to justice.

We have also created the National Cyber Force to help transform the UK's ability to counter and deter adversaries, and further our interests and promote our values.

We are also taking action to tackle the truly horrific levels of online child sexual abuse and exploitation, with law enforcement agencies, making an estimated 800 arrests and safeguarding or protecting over 1,000 children every month.

The key in all of this is to increase our resilience; from the most critical and important systems right through to PCs, tablets and smartphones – the very tools and devices used every single day – but to put the right protections in place to deliver on our ambition of making the UK the safest place to be online.

As a world-leading organisation in its field, the NCSC has a pivotal role to play, working across government and with industry to drive improvements in cyber security.

We have also set up the cyber Protect Network and Cyber Resilience Centres to boost the support provided by police to the public and businesses.

These are, of course, international issues. And that means the relationships we have with partners around the world, including our Five Eyes allies, are more important than ever before.

As I have set out, we are making progress. But we cannot stand still – this work is simply too important.

So we will, as promised in the Integrated Review, develop a comprehensive cyber strategy that will set out how we will maintain the UK's competitive edge and counter the threats from cyberspace.

In line with this ambition, it is critical that government has all the right levers available to ensure that those who commit criminal acts in cyberspace are effectively investigated by law enforcement, and prosecuted by our criminal justice system.

Including those perpetrating the most heinous and appalling crimes against children or those committing serious fraud.

The Computer Misuse Act has proved to be an effective piece of legislation to tackle unauthorised access to computer systems, and it has been updated a number of times to take account of changes we now face.

Alongside the Act, there is also separate legislation that provides powers for law enforcement agencies to investigate both cyber-dependent and cyber-enabled crimes.

As part of ensuring that we have the right tools and mechanisms to detect, disrupt and deter our adversaries, I believe now is the right time to undertake a formal review of the Computer Misuse Act.

And today I am announcing that we will be launching a call for information on the Act this year.

I would urge you all to provide your open and honest views on ensuring that our legislation and powers continue to meet the challenges posed by the threats in cyberspace.

Before I finish, I want to thank you again for the opportunity to speak to you today – and for all of the work that you do.

These are complex challenges, these are difficult issues, so it is absolutely vital that we work together closely to confront them.

We have made great strides, and we all know there is more to do.

My message to all of you working across the public and private sector to fend off cyber criminals and hostile state actors is simple: keep it up.

Your contributions and work are crucial if we are to stay one step ahead of our adversaries.

Ultimately, this is about keeping our citizens, our businesses, and our national security safe, and as Home Secretary that will always be my number one priority.

Thank you.