Minister’s speech at the NCSC Annual Review launch

Thank you, everyone, for joining us this morning. Cyber security is genuinely a massive priority for the government and it gives me great pleasure to launch the National Cyber Security Centre’s third Annual Review.

Now it took me around three seconds to say that. That’s not a very long period of time.

But in cyberspace, as you all know, an awful lot can happen in those three seconds.

Two hundred thousand and more Google searches made.

Eight and a half million emails can be sent.

Incalculable sums of money – not to mention priceless data – potentially lost to cyber criminals.

And there’s no reason in asking Alexa to help get it back, I’m afraid she’s not going to be of any help.

But we are very fortunate that we have a stronger ally than Alexa, and that is in the National Cyber Security Centre.

The Centre was created in 2016 and has helped make the UK safer.

Securing the internet is a 24/7 challenge, 365 days a year, in a complex landscape whose contours constantly change.

And in an area where success is measured in events that don’t happen – the dog that didn’t bark; the crippling cyber attack that wasn’t; the public trust in our digital systems that wasn’t compromised – we are, demonstrably, heading in the right direction.

A fifth fewer incidents of computer misuse were experienced by adults in England and Wales last year than in the previous twelve months.

The NCSC is working. And the government’s wider National Cyber Security Strategy is working too.

It is making citizens and businesses of all sizes safer.

It is making our data – an increasingly valuable asset – more secure.

And it is making our increasingly digitised government and critical national infrastructure stronger.

As Minister for the Cabinet Office, responsible for driving our ‘whole government’ approach to cyber security, I really am proud of what the NCSC

achieves for the United Kingdom every second of every day.

And you really don't have to take my word for it. After the NCSC's first two years, the Joint Committee on the National Security Strategy praised its 'impressive impact'.

And year on, there has been even more progress.

We live in an era when society relies on the internet as never before. A world-leading digital society like the United Kingdom is good for citizens in so many ways. It offers reliable access to information and markets of all kinds, and the ability to share data quickly and easily.

Almost every individual and organisation makes an online connection every single day. Some make literally thousands. With friends and families; customers and clients; with dogs via petcams and even with internet-enabled fridges that remind us we're low on milk.

Digital and mobile expansion, and the proliferation of the 'Internet of Things' devices in homes, workplaces, schools and hospitals, is happening fast – and so fast, however, that we risk leaving security considerations behind.

Not everyone is as conscientious as they should be about using a different password for each internet site, and I should say one not fashioned around their date of birth.

It's much easier and cheaper than ever for criminals to get hold of the tools to launch high volume, low-sophistication cyber attacks.

This perfect storm requires a co-ordinated fightback. The Government launched the National Cyber Security Strategy to counter these particular threats. And to achieve the best protection for the public, to uphold trust in our systems, and underpin future national prosperity and growth. In doing so we created a world-leading cyber authority.

But we want to go even further to harness the power of tech for the benefit of citizens, the economy and our democratic processes. And today we will hear about the difference the NCSC – as part of GCHQ – has made as a critical pillar of this government's security strategy and cyber ambitions – Ciaran has more details of some stand-out moments of this year.

The common theme of the NCSC's work, whether it's protecting critical national infrastructure or strengthening the security of the Internet of Things, is that it is rooted in cyber's increasing relevance to people's day-to-day lives. And it's precisely because cyber attacks affect everyone and the things that we value that we all need to play a critical role in protecting them.

Seen by other countries as a model of its kind, the NCSC's particular strength comes in fusing the cream of our national security capabilities with cutting-edge technical knowledge, and timely, tailored intelligence.

Its national and international projects and programmes take the fight to our cyber adversaries – hostile states; reckless hacktivists; and organised gangs.

In October 2018, that meant exposing Russian military attacks on political institutions and business, media and sporting interests – the World Anti-Doping Agency in Lausanne was a target. This week, it exposed how suspected Russian-based cyber hackers had piggybacked on the illegal operations and methods of a group of Iranian-led hackers, targeting 35 countries.

Domestically, the NCSC helps individuals spot where their own security needs to be tightened and shows them how to fix it. It is developing a pipeline of talent that will bring new ideas and abilities into an industry hungry for the best people. And in a cyber world with no frontiers, the NCSC is helping shape the global approach to cyber security by working with emerging nations.

Is there more to do? Of course, there is always more to do.

Over a third of UK businesses suffered a cyber breach or attack in 2018.

For this massively complex and evolving challenge there is no quick fix – we all need to step up, with the Government in the lead when a national response is appropriate.

We backed the Strategy with £1.9 billion of funding because this is the level of investment needed to protect what is a clear public good. We are acting on threats from hostile nation states, and also on lessons learned from previous attacks – for example, WannaCry, which disrupted the NHS in 2017. Our goal is to spare patients from the threat of cancelled operations and missed appointments, by working with the health services in Wales and Scotland, as well as England, to bolster their cyber security.

For similar reasons – to protect the public – we have also strengthened the resilience of government by using Active Cyber Defence measures that protect local authorities from harm at scale. By using Cloud services in public services, we can move on from insecure legacy systems. This kind of digital transformation allows us to use Government data more flexibly, in a way that streamlines and improves the online services citizens enjoy.

No less important, in protecting citizens, is the government’s work to protect the integrity of elections through our Defending Democracy programme – upholding public trust and helping to promote open dialogue online and elsewhere.

But the arms race between criminals and IT security is never-ending. The government cannot compete on its own and have any hope of a win.

We really do need to build even closer relationships with industry and society in this country and internationally, so that together we create those robust defences – combining the best ideas with the most effective enforcement tactics.

And this is the motivation for the current DCMS review of regulations and

incentives around cyber security: to make very sure that when the Government intervenes, it does so in a way that actively helps organisations overcome barriers by protecting themselves online, and makes good cyber security a market norm.

None of this progress would be possible without our stakeholders and I really am delighted that many partners in our cyber transformation have joined us this morning.

If the National Strategy reflects one core message, it is that cyber security is for everyone.

Sole traders as much as FTSE100 giants.

People who watch Netflix box sets on iPads as much as big employers with armies of IT technicians.

This winter, we relaunch Cyber Aware – the government's national cyber security campaign – informing the public about what they need to do to protect themselves from cyber crime.

We will carry our fair share, and more, of the cyber security load wherever possible. But everyone has their part to play.

When we work together to plug the gaps, the UK will continue to maximise the benefits of the digital economy. And the legacy of the cyber security strategy will be a world-leading system of defence that endures well beyond its initial, five-year lifespan.

We see in the NCSC and the Cyber Security Strategy the best traditions of its parent body, GCHQ, over its 100-year history. It has evolved to tackle the most serious criminal, and state threats. Among these, cyber threats will continue to evolve as new technologies emerge, and our adversaries become more capable.

It is certainly the case that the money we have invested in extra capacity and fixing structural issues will take more time to show results.

We are continually refining what we do, and there are always ways that we can improve.

That nearly one million adults were on the wrong end of computer misuse last year shows there is much work still to be done.

But when we set up the NCSC as part of the GCHQ family, it was to help make the UK the safest place to live and do business online.

It was to empower people to play their full part in our national security, showing them how to better protect themselves and each other.

And to bring together in one place the skills, talent, innovation and research we need.

The NCSC is showing its worth across the board and across the whole of society. And I look forward to it continuing to shape and strengthen our cyber defences now and in the future.

Thank you.