[Speech: Chancellor's speech at the National Cyber Security Centre opening](#)

It is a pleasure to be here today at the launch of the [National Cyber Security Centre](#), having been involved in this project, in various roles, since its inception.

In my current role, as Chancellor, I know how much the internet revolution has transformed our economy. And how much it holds the promise of future growth and prosperity for our country.

But as we enter the so-called 'Fourth Industrial Revolution', we have to be alive to the fact that this transformation is not without its challenges.

The development of artificial intelligence heralds a technological revolution that will fundamentally change our lives.

But it will also disrupt existing patterns of work, life, and society.

The fact is that the greater connectivity that will enable the development of the digital economy. Is also a source of vulnerability.

And those who want to exploit that vulnerability have not been idle.

The cyber attacks we are seeing are increasing in their frequency, their severity, and their sophistication. In the first three months of its existence, the NCSC has already mobilised to respond to attacks on 188 occasions.

And high-profile incidents with Sony, TalkTalk, and TV Monde have reminded us of the scale of damage that a single successful cyber-attack can inflict.

So this new centre, and its work, is vitally important.

This is a unique institution.

Our overseas competitors can only dream of the level of interagency cooperation that underpins it.

And we in Britain can be extremely proud to be blazing a trail that others will surely follow.

There are three key points to make about the way the centre will approach its task.

First, it will not just focus on protecting against major attacks on critical national infrastructure, but also raising our security capability against day to day malicious cyber activity.

The most dramatic threats are the high-end sophisticated state-sponsored

attacks.

But the most common threat that businesses and the general public face are the less sophisticated, mass targeted attacks, from phishing to email viruses.

83% of UK businesses are online.

The average British home has 8 devices connected to the internet.

This provides enormous potential for day to day attacks, from electronic data theft to online ransom.

The ONS estimate that there were two million such incidents in the past twelve months alone.

If these numbers were included in our crime figures, the UK's crime rate would double.

So the NCSC will play a unique and crucial role bringing together the public and the business community on the one hand, and our intelligence and security agencies on the other.

Second, it will focus on partnership.

Our intelligence and security agencies are the best in the world. No question.

Our digital sector is also the best in the world — contributing a bigger proportion of our GDP every year than any other country in the G20.

And to prove it we have the highest proportion of online shoppers in Europe.

And what we are doing here is, bringing them together, this centre will work hand in hand with industry to keep the UK safe.

65% of large businesses reported a cyber breach or attack in the past 12 months.

Yet nine out of ten businesses don't even have an incident management plan in the event of a cyber breach. Business has to sharpen its approach as the scale of the threat from cyber increases and intensifies.

Just as you would expect a shop on the high street to fix its locks and burglar alarms, so businesses operating digitally need to fix their online security.

And this Centre stands ready to help them in doing that.

It can be as simple as providing guidance on things like ransomware and device security so that the public and businesses can protect themselves.

Or it could be drawing on our most sophisticated capabilities to road-test and make available safeguards against more sophisticated threats.

Or mobilising the resources of public and private sectors to intercept, defeat and mitigate the effects of a concerted cyber assault.

Either way, its success will rely on partnerships.

The third and final point I want to make is that we are prepared to invest the necessary resources to get this right.

We invested £860 million on enhancing our cyber defences in the last Parliament.

And we are investing another £1.9 billion to further bolster our armoury against cyber-attack in this Parliament, as well as developing our offensive cyber capability to deter, and if needs be, retaliate against, those who seek to do us harm in cyberspace, a new and critical domain of our defence.

And all this is set in the context of our commitment to meeting the NATO pledge to spend 2% of our national income on defence for every year of this decade.

At the beginning of this month, the UK signed the NATO Cyber Defence Memorandum of Understanding so that we can share our expertise with our international allies, and learn from their experiences.

And today I am delighted to announce a new kind of partnership, closer to home, here at this centre.

We will invite business to second up to 100 employees to come and work in the NCSC – allowing us to draw on the best and the brightest in industry – to test and to challenge the government's thinking as we take this project forward.

And for these people to then return to the private sector and draw on their experience at NCSC to drive change within industry.

Because the government cannot protect businesses and the general public from the risks of cyber-attack on its own.

It has to be a team effort.

It is only in this way that we can stay one step ahead of the scale and pace of the threat we face. I want to thank the staff here at the Centre for their dedication, commitment, and skill.

And I want to thank our industry partners for teaming up with government, to ensure that the UK becomes truly, the safest and most secure space for digital business.

Thank you.