Security Minister’s speech to CYBERUK 2026

22.4.2026 - | Her Majesty's Revenue and Customs

Security Minister Dan Jarvis MBE uses speech at CYBERUK to say AI companies should work with government in a “generational endeavour”.

Good morning.

We find ourselves today at a profound technological crossroads in cyber and AI.

And to navigate it, we need a spirit of fearless innovation.

So it is fitting that we are gathered here in Glasgow,

a city that has long served as the engine of human progress and resilience.

We stand in the home of world-changing breakthroughs, and no, I’m not just talking about Chicken Tikka Masala!

I’m talking about Artificial Refrigeration, first demonstrated by William Cullen,

Antiseptic surgery, introduced by Joseph Lister,

Clean water, when James Morris Gale engineered the city’s resilient water system,

All three didn’t simply respond reactively to threats.

They built new resilient systems for preventing the threat in the first place.

This spirit of innovation is alive today.

Stand on the banks of the Clyde, just a few miles from here, and you are standing on the ground where the modern world was — and still is — being built.

We rightly celebrate the history of this great river.

But Clyde shipbuilding is not just a proud legacy;

it is a world-leading, modern-day success story.

Steel, sweat and engineering brilliance, pouring out of this city and into every ocean on earth.

“Clyde-built” doesn’t just mean a ship.

It means a standard.

That tradition of industrial courage — of meeting the demands of a new and dangerous world head-on — is why we are here today.

Because this city has always understood that the security of a nation is inseparable from its capacity to build.

Almost exactly 44 years ago today, a piece of plastic and silicon the size of a hardback book was

released to the British public.

The ZX Spectrum.

For those who might not remember it, sadly, I do, it was the UK's first truly affordable mass-market home computer.

It inspired a generation of bedroom coders, engineers, and digital pioneers — the people who built the British digital economy.

But forty-four years later, the world they built is being weaponised against us.

Before I came into politics, I served in the Armed Forces.

The threats I trained to face at Sandhurst were physical.

If an adversary wanted to strike Britain, they had to cross water.

But as the Prime Minister has said, we are living in an era of geopolitical instability not seen for a generation.

The nature of the threat has changed and the nature of warfare has changed with it.

Attacks on British systems are increasing in volume, in sophistication, and in ambition.

They come from criminal syndicates operating across borders, from ransomware gangs who treat children's nurseries as targets of opportunity, and yes — they come from hostile states.

States that have concluded the most effective way to weaken this country, is not to confront us directly, but to quietly hollow us out.

To hack the logistics systems that move our goods.

To compromise businesses that keep our high streets alive.

Think about the recent attack on Jaguar Land Rover and the damage it inflicted on their business.

If this damage had been caused by an old-school, physical attack it would have been the equivalent of hundreds of masked criminals turning up to dealerships across the country breaking glass, smashing up computers and driving cars right off the forecourt.

The truth is, there is no significant difference between these types of attacks — they are both brazen acts of criminality.

NCSC handled over 200 nationally significant incidents last year.

More than double the year before.

That number tells me the frontline isn't coming — it's here.

So I want to make something very clear today: The cyber security of British business is a matter of national security.

Now. I want to be direct about what this means in practice.

The government’s role is to set the standard.

To share the intelligence.

To build the support and provide the guidance.

What it cannot do —what no government can do — is substitute for the decisions that every organisation and business in this country needs to make.

Basic cyber hygiene is no longer optional, but the baseline — the absolute minimum we should expect of any serious organisation operating in the modern economy.

And if we are asking that of you — then we also have a responsibility to you.

Which is why today I am announcing a new

£90 million investment to strengthen our cyber resilience.

We will provide practical, targeted support to help our small and medium-sized businesses

And we will boost cyber resilience in priority areas.

We will help organisations implement the Cyber Essentials standard and are also asking every major organisation to sign a new Cyber Resilience Pledge which we will launch this summer.

The Pledge invites organisations to make a public commitment, to their investors, their customers, their supply chains, to make cyber security a Board responsibility to sign up to the NCSC’s Early Warning service to demand that your suppliers are Cyber Essentials certified.

And to encourage these actions within your own supply chains.

This will signal that cyber security is taken seriously at the highest level.

Companies that sign the Pledge will be listed online and highlighted as exemplars of good practice.

All this action will be detailed when we will publish the full National Cyber Action Plan this summer, setting out our vision and concrete actions for government to take alongside businesses.

The plan will demonstrate how we will tackle the growing threat, how we will strengthen our collective resilience, and how we will harness the opportunity for our world-leading cyber sector to secure the UK’s economic growth for years to come.

The nature of the threat is changing faster than any previous government has had to confront.

AI is lowering the barrier to entry for our adversaries.

It is automating attacks.

It is finding vulnerabilities in critical systems faster than any human team can patch them.

We cannot fight a machine-speed threat with human-speed bureaucracy.

Just this month, we saw the revelation of Anthropic’s new Claude ‘Mythos’ AI model.

In testing, it autonomously found thousands of zero-day vulnerabilities across major operating

systems.

It uncovered critical flaws that had gone unnoticed by human experts and automated tools for over two decades.

Neither industry nor government can close that gap on their own.

Government has something industry cannot replicate — sovereign classified intelligence, the deepest picture of the threat landscape, built over decades.

And the people in this room have something that government cannot replicate: the speed of the market, commercial agility, and the engineering talent to build at scale.

In short, we need to work together, and we're wasting no time.

Our world leading AI Security Institute tested Mythos and is working directly with a range of companies on Frontier AI.

In a joint public letter issued last week, the Secretary of State for Science, Innovation and Technology and I urged businesses to take specific actions to strengthen their cybersecurity.

The Secretary of State is meeting with major UK firms and cyber defenders.

And we're making the UK one of the most attractive places in the world to work on AI.

Just last week Open AI announced it was choosing the UK for its first permanent home outside the US, joining DeepMind, Meta, Synthesia, Wayve.

Anthropic has also announced a major expansion of its own operations in the UK, scaling up to accommodate 800 employees.

But we must go further.

The recent leap in frontier models means agentic AI has arrived.

The frontier labs driving this innovation are pushing the boundaries of human capability.

We are already seeing them bring new commercial defensive tools to the market to help mitigate these emerging risks.

For the broader economy, these tools are highly valuable.

But let me be clear: protecting Critical National Infrastructure requires a fundamentally different approach.

We will not secure the central pillars of the UK state simply by purchasing off-the-shelf vendor solutions.

We need a new model of collaboration, and it is time to set a higher standard for responsible action.

Today, I can give a commitment that the government will respond to this changing threat.

We will need to build national scale, AI powered cyber defence capabilities.

Capabilities that can protect our nation's most critical networks by autonomously identifying and addressing vulnerabilities at a speed and scale no human can match.

To achieve this, my message to the frontier AI companies is this: true responsibility goes beyond releasing enterprise software.

We want you to work with us directly.

Partner with the UK Government to co-develop AI for national cyber defence.

And make no mistake — this is a generational endeavour, and it will test the absolute limits of our engineering and innovation.

We are currently laying the groundwork for this national capability, and we will be setting out our formal agenda in due course.

We know where we are going.

We are inviting the pioneers of this technology to step up, share the responsibility, and help us build it.

I want to leave you with this.

Our resolve — genuine, collective, sustained resolve —changes the odds.

Whether you are a sole trader, a supplier to an NHS trust, or the CTO of a multinational — you are part of our national defence.

The actors will adapt.

The threats will evolve.

But if we follow the example of Cullen, Lister and Gale and build preventative systems, take shared responsibility for our digital borders, and match their speed and ambition with our own.

We will ensure that this country remains one of the most prosperous and resilient nations in the world, honouring that "Clyde-built" spirit of innovation.

Thank you.

https://www.gov.uk/government/speeches/security-ministers-speech-to-cyberuk-2026