Retaining defensive advantage in the age of frontier AI cyber capabilities

As AI accelerates vulnerability discovery, organisations must raise their security baselines to safeguard their cyber security.

> This blog post was originally published as a letter in the Financial Times 15th April 2026.

A step change in frontier AI models' capabilities to find vulnerabilities in code can ultimately be a good thing for our cyber security.

Suppliers of technology can use AI to identify and fix vulnerabilities in their products and services throughout their lifecycles, keeping customers and users safe from new threats. But the path to reaching this point brings significant risk and requires urgent action.

In the immediate term, we will increasingly see AI exposing those organisations that have not taken appropriate steps to safeguard their cyber security.

AI will make it easier, faster and cheaper to discover and exploit weaknesses that previously required more time, skill or resource for attackers to identify. And the pressure on organisations to patch systems quickly will only grow more acute.

That's why it is more essential than ever that organisations ensure they are following established good practices, set out by the National Cyber Security Centre, to raise their security baseline.

This includes reducing unnecessary exposure to attack, applying security updates rapidly, as well as monitoring for, and quickly responding to, malicious activity detected.

These are technical actions, but they must be championed by all leaders and board members at organisations to have a positive impact. Cyber risk is business risk.

A wealth of guidance and tools are available on the NCSC website to do this, and government-backed certifications such as Cyber Essentials give organisations and their customers confidence that critical disciplines are being practised.

As our society navigates these fast-evolving capabilities, the NCSC will stay focused on its mission to protect the UK from cyber threats, working alongside industry and wider government, and we will continue advising on the risks and opportunities.

By getting the fundamentals right and carefully adopting frontier AI models for good, network defenders can retain an advantage and help keep the UK safe online.

Dr Richard Horne, CEO NCSC

WRITTEN BY

Richard Horne
Chief Executive Officer (CEO)

PUBLISHED

15 April 2026

WRITTEN FOR

Cyber security professionals Large organisations Public sector Small & medium sized organisations

PART OF BLOG

Inside the NCSC