The Prime Minister
10 Downing Street, London SW1A 2AA

CC:
The Leader of the Opposition
The Secretary of State for Science, Innovation and Technology
The Shadow Secretary of State for Science, Innovation and Technology

Dear Prime Minister,

AI now poses substantial risks to our national security.

In February of this year, a lone criminal used commercially available AI tools to carry out cyber attacks on nine Mexican government agencies and exfiltrate hundreds of millions of citizen records. The UK's own AI Security Institute has found that Anthropic's latest model, Claude Mythos, can *"discover and exploit vulnerabilities autonomously – tasks that would take human professionals days of work."* And the offensive cyber capabilities of AI are rapidly progressing.

We depend on the functioning of computer systems in our critical infrastructure. Disruptions to those systems can threaten our drinking water supply, electrical grid, hospitals and financial services. The consequences of disruption can be severe and widely felt: the 2017 WannaCry attack forced the cancellation of 19,000 NHS appointments.

The Government's Cyber Security and Resilience Bill is a welcome step, but it places the burden of security primarily on the operators of essential services. AI developers whose models are used in cyber attacks must share some of the responsibility for minimising the risks that they create.

Moreover, cyber attacks are only the most visible threat. The International AI Safety Report 2026 found that current AI systems can already provide *"expert-level laboratory instructions"* for the creation of biological and chemical weapons. As AI capabilities advance, the range of potential catastrophic harms will expand. Many experts warn that developers may lose control of their own AI models if they succeed in creating systems that exceed human capabilities across all cognitive domains.

The UK has no specific legal standards for AI. No regulator oversees frontier AI development. And UK law does not reliably hold developers liable for damage or deaths caused by their models, even when the danger is predictable, preventable and uniquely enabled by AI. In short, UK law neither requires developers to guard against frontier AI risks, nor exposes them to any financial consequence if they fail to do so.

Given the pace at which AI capabilities are advancing, this matter cannot wait. We urge you to introduce legislation to address the risks of frontier AI development.

Yours sincerely,

To sign this letter, please email policy@pauseai.uk.