

UK cyber chief warns of a "perfect storm" as AI and geopolitics reshape cyber risk



The head of the UK's NCSC told CYBERUK that rapid AI-driven change and geopolitical tension are creating deep uncertainty, and called on organisations to make cyber security part of everyone's mission.

- Dr Richard Horne, CEO of the UK NCSC, spoke at CYBERUK in Glasgow on 22 April.
- He described rapid technological change plus geopolitical tension as "tumultuous uncertainty" requiring a cultural shift in cyber defence.
- The volume of incidents handled by the NCSC is fairly steady, but most nationally significant incidents now originate directly or indirectly from nation states.
- He said cyberspace sits between peace and war, and that cyber operations are now integral to conflict.

- Frontier AI is enabling discovery and exploitation of existing vulnerabilities at scale, exposing where cyber security fundamentals remain unaddressed.

What was said

Speaking at CYBERUK in Glasgow, Dr Richard Horne, CEO of the UK's National Cyber Security Centre (NCSC), said the country faces a "perfect storm". He pointed to the combination of a new technological revolution driven by AI and rising geopolitical tension, which he described as a period of "tumultuous uncertainty".

He argued that the scope of cyber security is widening. Securing technology that controls robotics, autonomous systems and devices integrated with the human body goes well beyond how the discipline was understood a decade ago, so organisations must keep reimagining it.

The threat picture

According to the speech, the number of incidents the NCSC handles is fairly steady, but their origin has changed: most nationally significant incidents now come directly or indirectly from nation states. He said cyberspace is part of a contested space between peace and war, that Russia is applying lessons from the battlefield in Ukraine beyond it, and that cyber operations are now integral to conflict.

On frontier AI, he said it is rapidly enabling discovery and exploitation of existing vulnerabilities at scale, which shows how quickly unaddressed fundamentals will be exposed.

Why it matters

His central message was cultural: cyber security is everyone's responsibility, from the Board to the IT help desk, and organisations that do not treat their technology base as core to their prosperity fail to grasp today's reality. Although the speech concerns the UK, the themes apply to any regulated institution that depends on digital services.

What to do now

1. Brief the Board and executive management on the link between geopolitical tension, nation-state activity and your own risk profile.
2. Review whether cyber security responsibilities are explicit for every role, from senior leadership to the service desk, and reinforce them through awareness programmes.
3. Verify fundamentals such as asset inventory, patching and vulnerability management, given AI-accelerated exploitation of known weaknesses.
4. Reassess threat models and incident response and recovery plans for state-linked scenarios, and test them in exercises.
5. Map these priorities to your NCA ECC and SAMA CSF control programme and record any gaps in the risk

register.