

UK NCSC Reports State Actors Behind 75% of Critical Infrastructure Cyber Incidents



The UK's National Cyber Security Centre managed over 200 cyber incidents affecting critical infrastructure in the year to May 2026, with three-quarters linked to hostile state actors including Russia, China and Iran.

- Over 200 cyber incidents affecting UK critical infrastructure managed by NCSC in the year to May 2026
- Approximately 75% of these incidents linked to hostile state actors including Russia, China and Iran
- NCSC CEO warns cyber security must be treated as an ongoing contest with capable adversaries, not merely a risk to manage
- AI-enabled cyber capabilities likely to be used at scale against legacy technology in critical infrastructure by 2028

- Organisations urged to focus on understanding threat exposure, building stronger defences, and ensuring operational continuity

State-Sponsored Threats Dominate Critical Infrastructure Attacks

The head of the UK's National Cyber Security Centre has disclosed that hostile state actors were linked to approximately three-quarters of cyber incidents affecting critical national infrastructure over the past year. Dr Richard Horne, NCSC CEO, revealed that the agency managed more than 200 such incidents in the year to May 2026, with Russia, China and Iran identified as key threat sources.

Speaking at the Royal United Services Institute's Annual Security Lecture, Dr Horne emphasised that **cyber security** should not be viewed simply as a risk management exercise but as an ongoing contest with capable adversaries. He noted that many significant incidents today remain possible because fundamental security controls are not in place, warning that vulnerabilities tolerated in peacetime will be exploited during conflict.

AI to Accelerate Threat Landscape by 2028

The NCSC assesses that by 2028, attackers will likely deploy **AI-enabled cyber capabilities** to exploit known vulnerabilities in legacy technology at scale across critical national infrastructure. Dr Horne stressed the urgency of action, arguing that organisations are already fighting tomorrow's conflicts in cyberspace today.

He called on every board member and executive to strengthen cyber resilience through three core capabilities: understanding exposure to threats, building stronger defences based on proven security fundamentals, and ensuring the ability to continue operating and recover quickly after an attack. The NCSC has published guidance to help organisations counter AI-powered attacks by improving foundational cyber security now.

What to do now

1. Review your organisation's exposure to state-sponsored threat actors, particularly those targeting critical infrastructure and essential services sectors
2. Assess and remediate fundamental security controls across your environment, prioritising known vulnerabilities in legacy systems before they are exploited at scale
3. Establish or strengthen board-level understanding of cyber security as an ongoing adversarial contest requiring continuous investment, not a one-time risk mitigation exercise
4. Develop and test operational continuity and recovery capabilities to ensure your organisation can maintain essential functions during and after a cyber incident
5. Evaluate your preparedness for AI-enabled attacks by 2028, focusing on automated exploitation of known vulnerabilities across your technology estate
6. Implement the three core capabilities outlined by NCSC: understanding threat exposure, building defences

based on proven fundamentals, and ensuring rapid recovery