Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: TA | AP Brief

The UK's critical infrastructure may be the target of AI cyberattacks by 2028



The U.K. will likely face artificial intelligence cyberattacks on its critical infrastructure by 2028 as criminals and states, including China and Russia, increasingly use AI in their cyber activity, Britain's cyber chief warned Tuesday.

That could include AI-powered malware for ransomware attacks as the technology will allow “vulnerabilities that have been tolerated for far too long” to be discovered and exploited “at a scale that was once unimaginable,” Richard Horne, the head of the U.K.'s National Cyber Security Center said.

In a speech marking the publication of the NCSC's annual cyber report, Horne said the leaders of businesses and organizations of all sizes who have "got away with tech on the cheap" will have to explain why “food isn't on the shelves, lights aren't on, businesses have gone under,” if they fail to invest in cybersecurity or update out-of-date technology.

Chinese cyber activity is the “most sophisticated and sustained cyber challenge facing the U.K.” while both Russia and China will routinely use AI to achieve their geopolitical goals, the report said. Russia is intentionally conducting cyber campaigns which fall below the threshold of armed conflict while Iran is carrying out attacks against the U.K. and targeting individuals who are a threat to the Iranian regime, Horne said.

The use of AI by states and criminals is highly likely to increase the scale and efficiency of hostile operations, but AI is more likely to be used to enhance and scale existing tactics and techniques rather than find brand new vulnerabilities, the report said.

Last week, governments and corporations worked on urgent security updates after the AI-assisted discovery of vulnerabilities in a programming language vital to 70% of websites globally.

Russia has already attacked critical infrastructure in Europe

The two critical flaws identified by AI could allow bad actors to get unauthenticated access to sites which, in theory, could allow them to control a web server remotely without needing a password.

Technology “underpins the automation of physical processes that are vital to modern life,” Horne said.

That includes, he said, electricity switching, sluice gates in water facilities, dam operations, manufacturing lines, heating and refrigeration controls.

The recent cyberattacks on refrigeration systems in French supermarkets showed how easily hostile actors could exploit civilian infrastructure, Horne said.

Russia's FSB security service was behind an attack on Poland's energy grid in December 2025

Russia has already attacked critical infrastructure in Europe, according to the U.K. and EU member states that said Russia's FSB security service was behind an attack on Poland's energy grid in December 2025.

If the attack had been successful, 500,000 people could have lost electricity during winter.

In the U.K., malicious cyber activity is costing organizations almost $20 billion every year, the NCSC said.

In 2025, the carmaker Jaguar Land Rover suffered more than $260 million in direct losses following a cyberattack which also hit suppliers and dented the U.K. economy.

“We need every organization in the UK to take action now. Not only to protect their customers, services and livelihoods, but because cybersecurity is now part of the front line defense of our nation,” said Anne Keast-Butler, director of GCHQ, Britain’s signals intelligence agency, which the NCSC is part of.

That includes implementing basic but effective cybersecurity measures such as making sure devices are up to date, limiting administrator access to systems and backing up important files and data, the NCSC said.