TA Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: TA | AP Brief

# Most serious cyberattacks against the UK now from Russia, Iran and China

The most serious cyberattacks in the U.K. are now carried out by hostile nations including Russia, Iran and China, the head of the U.K.'s National Cyber Security Centre (NCSC) will say in a speech Wednesday.

Richard Horne, the head of the NCSC — part of the U.K's signals intelligence agency GCHQ — will warn that the U.K. is living through "the most seismic geopolitical shift in modern history."

British businesses, he will say, need to prepare themselves to defend against cyberattacks because the U.K. could be targeted "at scale," if it became involved in an international conflict, according to a preview of his speech shared with reporters.

In recent months, authorities in Sweden, Poland, Denmark and Norway have all warned that hackers linked to Russia have targeted their critical infrastructure including power plants and dams.

Horne will say the NCSC currently handles around four "nationally significant" cyber incidents a week and while criminal activity, such as ransomware, remains the most common problem, the most serious threat comes from cyberattacks carried out directly or indirectly by other states.

In December, Blaise Metreweli, the head of Britain's Secret Intelligence Service, or MI6, said the world is more dangerous and contested now than it has been for decades and that the U.K. is operating in a space between peace and war.

"Let's be clear, cyberspace is part of that contest," Horne will say.

China's intelligence and military agencies display an "eye-watering level of sophistication in their cyber operations," while Iran is "almost certainly using cyber activity to support the repression of British individuals on our streets who are seen as a threat to the regime," Horne will say in his speech at the CyberUK conference in the Scottish city of Glasgow.

## Cyberattacks at scale

Moscow, meanwhile, is using tactics and techniques honed during its war in Ukraine and is "moving them beyond the battlefield," Horne will say, pointing to "sustained Russian hybrid activity" targeting the U.K. and Europe.

Companies, he will say, must learn how cyber operations have been used in conflict situations in order to boost their own resilience.

In a conflict situation, Horne will say, the U.K. would likely face cyberattacks at scale but — unlike with ransomware — companies will not be able to pay their way out in order to recover data and access to systems.

> Every organization needs to understand the full extent of the risk they face and improve their cyber defenses before it is too late

For that reason, he will say, every organization needs to understand the "full extent" of the risk they face and improve their cyber defenses before it is too late.

On Friday, Swedish authorities said that a pro-Russian group with links to Russia's security and intelligence services was behind a cyberattack on a heating plant last year.

Carl-Oskar Bohlin, Sweden's minister for civil defense, compared it to incidents in Poland in December, when coordinated cyberattacks hit combined heat and power plants supplying heat to almost 500,000 customers, as well as wind and solar farms.

Poland later said evidence indicated hackers were "directly linked to the Russian services." Norwegian authorities also warned that a hack in April 2025 which affected water flows from a dam was linked to Russia while in December, Danish authorities said another attack on a water utility company in 2024 left some houses without water.

The four cyberattacks are among more than 155 incidents of disruption — including arson, sabotage and espionage — linked to Russia or its proxies by Western officials and tracked by The Associated Press since Moscow's full scale invasion of Ukraine in February 2022.

Other incidents linked to Russia by European officials include an attack on German air traffic control, attempts to gain access to Signal and WhatsApp accounts belonging to officials and journalists and attempts by hackers linked to Russian military intelligence to steal users' sensitive data by exploiting a weakness in some internet routers.