Britain ‘must brace for more Iranian cyber attacks’

Former US security chief expects UK infrastructure to be targeted again, following unprecedented breach of power plant

Rozina Sabur

National Security Editor

Published 29 August 2026

Britain’s energy infrastructure could face further attacks from Iran, a former US cyber chief has warned.

The Telegraph revealed last week that hackers affiliated with Tehran shut down a British power plant for four days in an unprecedented cyber attack.

And Britain, the US and other Western allies should “expect attacks like this to continue” as Tehran ramps up its cyber warfare, according to Jen Easterly, the former director of the US cybersecurity and infrastructure security agency (CISA).

In an interview with The Telegraph, Ms Easterly said companies that failed to heed alerts from the Five Eyes intelligence network in particular would be seen as “low-hanging fruit”. Five Eyes is an alliance between Australia, Canada, New Zealand, the UK and the US.

She said: “They [Iran] will take opportunities to be able to go after critical infrastructure, particularly with respect to water [facilities] that are not very well resourced.

“If you have internet-facing infrastructure, that makes them more vulnerable [and] if you have default passwords … they’ll take advantage of it, you know, opportunistically, entrepreneurially.

“But I think we should absolutely expect attacks like this to continue on US and allied infrastructure, particularly where there’s low-hanging fruit, like internet-exposed infrastructure.”

However, Ms Easterly praised the work of the National Cyber Security Centre (NCSC), an arm of GCHQ, saying she had seen first-hand how it had worked on not just preventing intrusions, but on improving the “resilience” of critical infrastructure.

With Tehran under growing diplomatic and economic pressure amid its confrontation with the US and Israel, the regime has dramatically stepped up its cyber attacks on the West.

Intelligence officials describe Iran as a capable adversary in the online domain, with its cyber apparatus working in concert with its wartime aims.

Jen Easterly said ‘we should absolutely expect attacks like this to continue on US and allied infrastructure’ Credit: Kevin Dietsch/Getty Images

In the incident revealed by The Telegraph last week, hackers affiliated with the Iranian regime succeeded in closing down an energy facility in the UK.

Government officials described the facility as “small scale” and said it had no impact on the wider power grid, but the incident is believed to be the most successful cyber attack of its kind in Britain.

The shutdown is understood to have occurred at the same time as a series of attacks on US water infrastructure last month, which affected multiple states.

The FBI attributed the incidents to “malicious cyber actors”, but US government sources later confirmed to media outlets that the threat probably originated in Tehran.

Ms Easterly noted that while the US had not publicly attributed the water attacks to Tehran, “you could connect the dots” from the various advisory notices that officials had issued regarding cyber activity and tradecraft.

“I think if you talk to CISA or FBI or [the National Security Agency] NSA at the technical level, they would probably have some level of confidence about this being Iran,” she said. “But there have obviously been some political issues around the attribution so I think they’re sort of hedging a little bit on that.”

She added: “That said, none of this is surprising. Whether it’s the water systems across states in the US or a small energy company [in Britain]. I don’t think it was terribly impactful, but this is the Iranian playbook, right? Iran goes after critical infrastructure.”

Ms Easterly led CISA – the US equivalent to GCHQ’s NCSC and MI5’s National Protective Security Authority – for almost four years under Joe Biden.

She previously spent more than two decades in the US army and served as a counter-terror director during the Obama administration as well as holding senior roles at the NSA, including in its elite hacking team.

She warned that technological developments meant “AI-generated, step-by-step” instructions and shopping lists on how to build bombs could be produced easily, as well as potentially be used for “recruitment and radicalisation”.

The former cyber-security chief is also promoting an upcoming film, Midnight in the War Room, a documentary which draws on former intelligence leaders’ experience to explore a cyber conflict between nation states.