Smarttech
YOUR 24/7 SECURITY PARTNER

Iran-Linked Cyber Attack Disruption at UK Power Facility

Overview

Suspected Iran-linked hackers took a small UK gas-fired power generation site offline for four days in late July 2026, the first confirmed case of an Iran-linked attack disabling a UK electricity generator. The incident ran alongside a separate, larger Iran-linked campaign that disrupted operational technology at water and wastewater utilities across at least 12 US states over the same period.

Both incidents sit within a wider rise in Iran-aligned cyber activity since US and Israeli strikes on Iranian targets in February 2026. The NCSC reports that hostile states, including Russia, China and Iran, were behind around 75% of the more than 200 nationally significant critical national infrastructure incidents it handled in the year to May 2026. The tactics used (scanning for internet-exposed controllers, default credentials) match a pattern IRGC-aligned groups, including the group publicly known as CyberAv3ngers, have used against Western operational technology since 2023. These operations are more often intended to demonstrate reach than to cause physical harm.

UK and US officials confirm neither incident affected wider grid stability or drinking water safety. The real message for clients is about exposure, not exploit sophistication: default credentials and internet-facing controllers were enough for state-aligned actors to force real operational disruption at both sites. This is a fixable attack-surface and resilience gap, not a problem that needs new tooling to solve.

Note: Both incidents were contained to isolated, small-scale sites. Attribution to a specific named threat group for the UK incident is not yet confirmed by UK officials. No confirmed impact to the wider UK grid or to US drinking water safety.

Threat Actor Profile & Attack Vectors

Threat Actor / Campaign Name

Officials have not named a specific group behind the UK power plant incident, describing it only as “Iran-linked.” The concurrent US water-sector campaign matches the tactics, techniques and procedures of IRGC-affiliated actors tracked by CISA, the FBI and the NSA, including the group publicly known as CyberAv3ngers, assessed as linked to the IRGC Cyber Electronic Command. CISA's advisory AA26-097A, updated 22 July 2026, covers the wider campaign against internet-connected programmable logic controllers.

Primary Attack Vectors

1. **Internet-exposed OT/ICS devices:** PLCs and human-machine interfaces (HMIs) at small-scale generation and water sites, reachable directly from the public internet without a VPN or an authenticated jump host in front of them.
2. **Default or reused credentials:** vendor default logins, first seen at scale on Unitronics PLCs in 2023 and 2024, now extended to Rockwell Automation/Allen-Bradley, Schneider Electric and Siemens controllers per CISA's July 2026 update.
3. **Opportunistic, low-sophistication targeting:** actors scan broadly for exposed controllers rather than building bespoke exploits, consistent with independent OT security research on this campaign.

4. **Loss of remote monitoring and control:** successful access lets attackers manipulate or disable pumps, valves, pressure and generation controls, forcing operators onto manual fallback.
5. **Tampering with reusable PLC code modules:** CISA's July 2026 update flags detection of malicious changes inside reusable code blocks within PLC logic, a more persistent technique than credential abuse alone.

Mitigation & Safeguards Matrix

The following maps each identified attack vector directly to CISA and NCSC recommended controls.

Focus Area	Identified Threat Vector	CISA / NCSC Recommended Control
Network Segmentation	OT devices (PLCs, HMIs) directly reachable from the public internet	Remove direct internet connectivity to OT. Enforce IT/OT segmentation with firewalls, a demilitarised zone (DMZ) or data diodes, per CISA and NCSC CNI segmentation guidance.
Identity & Access	Default, shared or weak credentials on PLC and HMI accounts	Replace default vendor credentials with unique, strong passwords per device. Enforce MFA on remote engineering access and apply least-privilege account design, per CISA AA26-097A and NCSC identity guidance.
Perimeter Security	Exposed remote-access pathways and unmanaged edge devices	Harden and patch edge devices and VPNs. Disable unused remote services (for example, direct VNC or RDP into OT). Enrol in NCSC's Early Warning service for external attack-surface alerts.
Monitoring & Detection	Loss of visibility into control functions; tampering with PLC code modules	Deploy OT-aware monitoring and logging. Review vendor-issued indicators of compromise and baseline PLC logic to detect unauthorised changes, per CISA AA26-097A.
Incident Response & Resilience	Operational disruption requiring manual fallback	Maintain and test manual-operation fallback procedures. Run OT-specific incident response and business continuity plans. Report incidents promptly to the NCSC or CISA.

Recommendations

1. Map the external attack surface. Identify every internet-facing OT/ICS asset (PLC, HMI, RTU) using external scanning tools or NCSC's free scanning services.
2. Rotate default and vendor-supplied OT credentials on every asset identified.

3. Confirm segmentation. Verify no OT asset is directly reachable from the public internet without an authenticated jump host.
4. Brief operations staff and validate that manual fallback procedures are current.
5. Patch and harden PLCs per manufacturer guidance referenced in CISA AA26-097A (Rockwell Automation/Allen-Bradley, Schneider Electric, Siemens).
6. Threat-hunt for the indicators of compromise published in CISA AA26-097A across OT and IT boundary logs.
7. Reset credentials and enforce MFA on all remote-access and engineering-workstation accounts.
8. Review and formally document every third-party and vendor remote-access pathway into OT.
9. Extend continuous monitoring and MDR coverage into the OT environment where feasible.
10. Align the resilience programme to the NCSC Cyber Assessment Framework and CISA's Cross-Sector Cybersecurity Performance Goals.
11. Run tabletop exercises simulating OT disruption and manual failover.

References

https://www.theguardian.com/world/2026/aug/23/iran-linked-hackers-blamed-cyber-attack-british-power-plant
https://www.bbc.com/news/articles/ce9793g34yvo
https://www.cnbc.com/2026/08/23/small-uk-power-plant-shut-down-after-iran-linked-cyberattack-report.html
https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a
https://www.cisa.gov/news-events/news/cisa-fbi-epa-and-us-government-partners-update-warning-iran-affiliated-threat-actors-targeting
https://www.cbsnews.com/news/more-states-water-systems-cyberattacks-iran-backed-hackers/
https://therecord.media/iran-cyberattacks-water-treatment
https://www.csis.org/analysis/mapping-iranian-cyberattacks-us-water-systems
https://www.csis.org/analysis/iranian-cyber-threat-us-critical-infrastructure
https://www.ncsc.gov.uk/news/ncsc-ceo-hostile-states-linked-to-three-quarters-of-cyber-attacks
https://www.cnn.com/2026/07/31/politics/sweeping-cyberattack-us-water-systems

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com