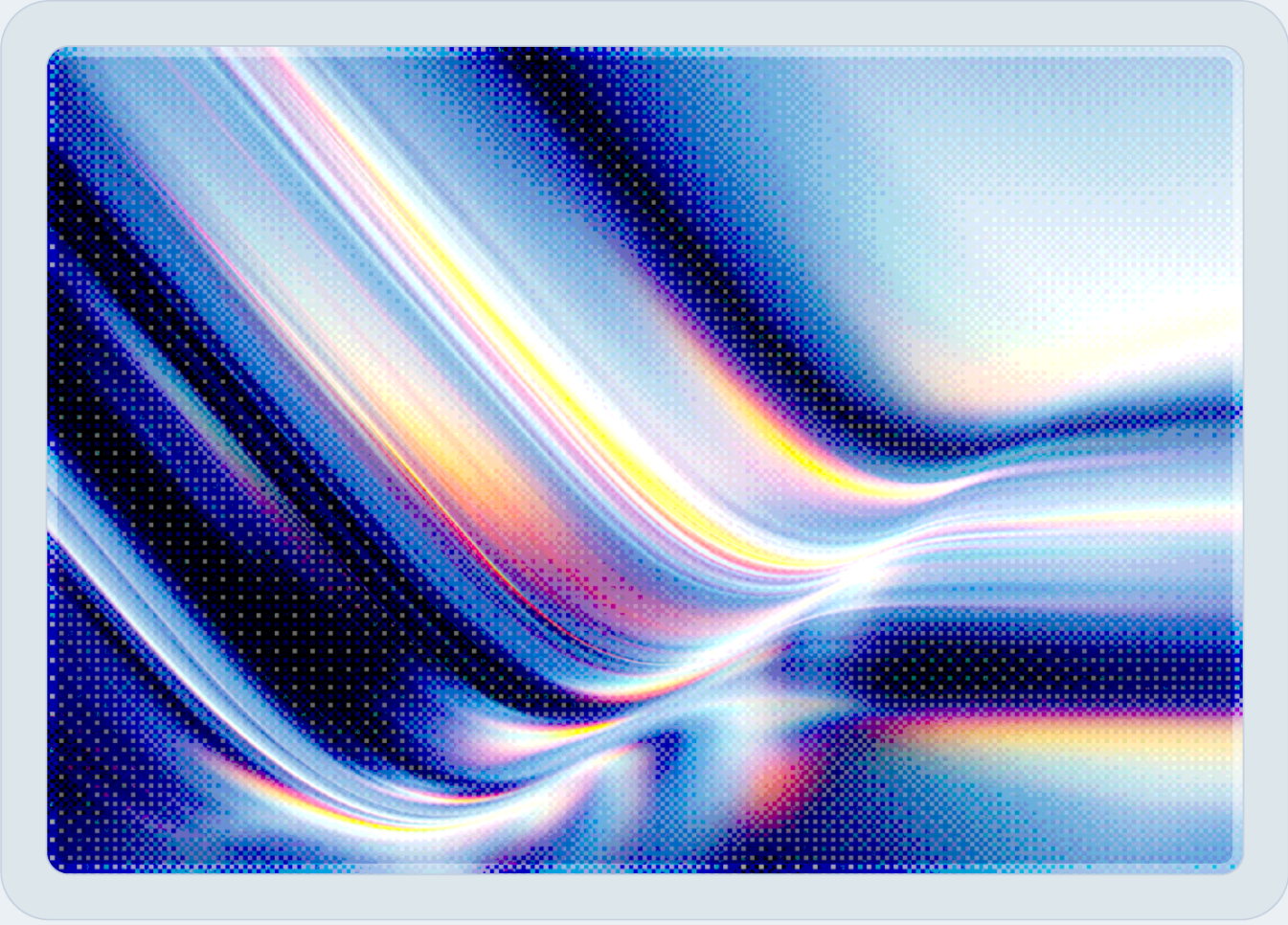
CSAI Foundation | Cloud Security Alliance

Iran-Linked Actors Hit UK Power and US Water Systems

2026-08-28

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

An Iran-linked intrusion knocked a British power plant offline for four days — an incident UK officials called unprecedented for the country's energy sector — in a window that overlapped with a broader campaign against water and wastewater utilities across at least twelve US states [1][2]. Together, the two campaigns represent the most significant concurrent transatlantic OT targeting publicly attributed to Iran-linked actors to date, though neither individually surpasses the scale of the 2023-2024 Unitronics campaign in device count. Both intrusion sets exploited the same class of weakness: internet-exposed programmable logic controllers (PLCs), often reachable directly through cellular modems or default credentials rather than through any hardened remote-access path. US federal agencies had already warned about this exact exposure in an April 2026 joint advisory, and the July-August 2026 events show that warning was not acted on broadly enough before attackers capitalized on it. The UK incident did not affect the wider national grid, and none of the US water incidents produced confirmed contamination, but both cases demonstrate that small, under-resourced OT operators remain the path of least resistance for actors seeking to demonstrate the ability to reach and briefly disrupt critical infrastructure. Security leaders should treat this as validation that PLC internet exposure is an active, exploited-in-the-wild risk category, not a theoretical one, and should prioritize remediation accordingly in the coming months.

Background

On August 22, 2026, The Telegraph disclosed that Iran-linked hackers had shut down a small British power plant for four days, an incident UK officials described as unprecedented for the country's energy sector [1][2]. The facility was not publicly named. A UK government spokesperson said the outage did not affect the broader UK power supply — an assessment shared by outside security researchers who reviewed the incident — though the National Cyber Security Centre (NCSC), which was informed of the incident, declined to comment on the facility's identity [2][3]. Security researchers who reviewed the incident characterized the underlying intent as demonstrative rather than destructive: gaining and proving persistent access to UK infrastructure, and showing the ability to interrupt it, appears to have mattered more to the intruders than causing lasting physical or economic harm [1][3]. That framing matches a pattern security vendors have tracked in Iranian-affiliated OT operations going back several years, in which access and disruption serve as strategic signaling as much as tactical objectives.

The UK disclosure landed in the same window as a sustained campaign against US water and wastewater utilities that had been building since late July 2026. Reporting first surfaced attacks on facilities in Minnesota before authorities confirmed that dozens of utilities across at least twelve states — including Michigan, Georgia, South Dakota, New Jersey, and Alabama — had experienced intrusions that caused loss of water pressure, flooding, and, in some cases, boil-water notices [4][5][6]. The Cybersecurity and Infrastructure Security Agency (CISA) told reporters that more than one hundred internet-exposed OT systems in the water sector had been affected, with PLCs connected directly to cellular modems identified as the common entry point [5]. CISA urged utilities to remove publicly exposed PLCs from the internet immediately and to route any remote access through a VPN or gateway rather than exposing controllers directly [5][7].

Neither campaign emerged without precedent. Six federal agencies — the FBI, CISA, NSA, EPA, the Department of Energy, and US Cyber Command — had issued a joint advisory on April 7, 2026, warning that Iranian-affiliated actors were actively exploiting internet-facing PLCs, including devices from Rockwell Automation/Allen-Bradley, across water, energy, government, and manufacturing environments [7][8]. That advisory followed years of activity attributed to CyberAv3ngers, a group formally tied to the Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC), whose officials the US Treasury sanctioned in February 2024 [9]. CyberAv3ngers previously compromised at least seventy-five internet-exposed Unitronics PLCs in 2023-2024, including at the Municipal Water Authority of Aliquippa, Pennsylvania, and at an Irish water utility that suffered a multi-day outage [9]. By 2026, the group had progressed from default-credential exploitation to deploying a custom Linux malware platform, IOCONTROL, capable of running on PLCs, routers, HMIs, IP cameras, and fuel-management systems from a wide vendor set, and had begun exploiting a known Rockwell authentication-bypass vulnerability, CVE-2021-22681, at scale [9]. Escalation in the group's operational tempo has also tracked geopolitical events; researchers noted intensified activity within days of the February 2026 US-Israeli strikes on Iranian nuclear facilities, and suspected Iranian OT operations were also reported in Germany, Poland, Finland, Belgium, and Albania during the same period [3].

Security Analysis

The UK power plant intrusion and the US water campaign can be read as expressions of a single underlying exposure rather than as two unrelated events, given that both rely on the same class of weakness: PLCs and other OT devices reachable directly from the public internet, frequently through undocumented or forgotten access paths such as cellular modems added for vendor convenience or remote maintenance [5][9]. This is a known, previously flagged weakness. CISA's April 2026 advisory explicitly named insecure remote access, credential compromise, and limited visibility into legacy or hybrid OT environments as the primary risk vectors for exactly this kind of attack [7][8]. That the

campaign nonetheless reached over one hundred water systems and disabled a UK generation asset for four days suggests that the April 2026 advisory's guidance had not been broadly implemented at the operator level by the time of the July-August incidents — whether due to lack of awareness, resource constraints, or incomplete remediation is not established by available reporting, but the pattern is consistent with the smaller, rural, and resource-constrained utilities identified in most of the affected incidents [4][5].

The asymmetry in outcomes between the two campaigns is instructive. The US water attacks caused operational disruption — loss of pressure, flooding, reversion to manual operations — without producing any confirmed water contamination. Affected utilities were able to isolate compromised control loops or fall back to manual processes once anomalies were detected, which appears to be a significant factor in the absence of confirmed contamination, though the sources do not rule out other contributing factors such as limited attacker dwell time [5][6]. The UK power plant recovery, by contrast, took four full days, prompting UK security researchers to question publicly why recovery at a plant of that size took so long and whether smaller energy operators are adequately prepared to detect and expel an intruder once initial access is achieved [3]. Both incidents point to the same underlying gap: in both cases, prevention (keeping PLCs off the internet) failed before detection and recovery capability was tested, and in the UK case even recovery took an extended period. Whether this reflects a sector-wide pattern beyond these two incidents would require broader data than is available here.

Attribution in both cases rests on a mix of technical indicators and circumstantial timing rather than a single definitive disclosure. US officials described the water campaign's origin as "most likely" Tehran, and CyberAv3ngers has not been formally and publicly named as the actor behind the July 2026 water intrusions in the way it was named for the 2023-2024 Unitronics campaign [4][9]. UK officials have likewise not issued a formal state-attribution statement tying the power plant incident to a specific IRGC unit, and one security researcher was quoted as saying that public attribution to hacktivist branding alone "probably isn't enough in geopolitics" when weighing a response [3]. This attribution ambiguity is itself a feature of how IRGC-linked operations are structured: campaigns are frequently run under hacktivist-style branding that provides Iran with a degree of deniability while still allowing the government to benefit from the deterrent and signaling value of demonstrated access to Western infrastructure [1][3][9]. Security teams should treat the ambiguity as a characteristic of the threat actor's operating model, not as a reason to discount the state-linked nature of the activity.

Recommendations

Immediate Actions

Critical infrastructure operators — and particularly small water utilities and distributed energy generation sites, which both incidents show are treated as lower-hanging targets than large national operators — should conduct an immediate inventory of every PLC and OT device reachable from the public internet, with specific attention to cellular modems and other remote-access hardware that may not appear in existing network diagrams [5]. Any PLC found directly exposed should be taken off the internet immediately and, where remote access is operationally necessary, routed through a VPN or dedicated secure gateway rather than exposed directly, consistent with CISA's guidance [5][7]. Organizations running Rockwell Automation/Allen-Bradley or Unitronics controllers should confirm patch status against the vulnerabilities named in CISA's April 2026 advisory, including CVE-2021-22681, and rotate any default or reused credentials on OT devices [7][9].

Short-Term Mitigations

Utilities and energy operators should validate that manual-operation fallback procedures are current, tested, and known to on-shift staff, since the ability to revert to manual control appears to have been a decisive factor in preventing the US water intrusions from causing contamination [5][6]. Organizations should also review incident recovery timelines against the four-day UK outage as a benchmark and identify what would slow their own recovery — asset documentation gaps, unclear escalation paths, and unfamiliarity with OT-specific forensics are common causes cited by researchers reviewing the UK case [3]. Establishing or refreshing relationships with sector-specific information sharing organizations, and confirming that OT incident response plans include a path to CISA and equivalent national authorities, will shorten the time between detection and coordinated response.

Strategic Considerations

Boards and executive leadership overseeing critical infrastructure operators should recognize that Iran-linked OT targeting is now tracking geopolitical events on a short lag, with operational tempo rising within days of regional military developments; security investment and staffing levels should be planned with that volatility in mind rather than treated as a static baseline risk [3][9]. Because IRGC-linked campaigns are frequently conducted under hacktivist branding to preserve deniability, organizations should build attribution ambiguity into their governance and disclosure processes rather than waiting for definitive state attribution before treating an intrusion as a national-security-relevant event [1][3].

Finally, the persistent gap between what federal advisories recommend and what has actually been implemented at the operator level — evident in the fact that the April 2026 joint advisory predated the July–August incidents by months — suggests that regulatory or assurance mechanisms with teeth, rather than advisory guidance alone, may be necessary to drive remediation at smaller, resource-constrained utilities.

CSA Resource Alignment

CSA's Zero Trust Guidance for Critical Infrastructure is the most directly applicable CSA artifact to this incident set. The guidance's five-step implementation process — defining the protect surface, mapping operational flows, and building zone-and-conduit segmentation around OT assets — addresses precisely the exposure pattern seen in both the UK and US incidents, where PLCs were reachable from the internet without an intermediating policy enforcement point. The guidance reports baseline statistics indicating that roughly a quarter of industrial sites maintain direct internet connections and over half have remotely accessible devices — figures that describe the same exposure class CISA identified as the entry point for the July 2026 water campaign, reinforcing that this is a known, chronic gap rather than a novel discovery.

CSA's State of ICS Security in the Age of Cloud provides useful historical grounding, having cataloged prior nation-state and criminal disruptions of ICS environments — including Iranian-attributed activity — and having flagged IT-OT convergence and legacy system exposure as structural risk factors well before the 2026 campaigns unfolded. Its analysis of how cloud-based monitoring and Zero Trust network segmentation can improve visibility into distributed OT assets is directly relevant to the smaller, rural utilities that made up most of the water-sector victims, since smaller utilities are widely reported to operate with limited dedicated security operations staffing compared to large utilities, and may benefit from managed or cloud-delivered monitoring capabilities that do not require in-house SOC investment.

References

[1] Pierluigi Paganini. "UK Power Plant Disabled for Four Days by Iran-Linked Hackers, Concurrent with U S Water Attacks." Security Affairs, August 2026.

[2] SecurityWeek Staff. "Iran-Linked Hackers Shut Down UK Power Plant for Four Days." SecurityWeek, August 2026.

[3] SC World Staff. "Iran-linked hackers target UK power plant and US water infrastructure." SC World, August 2026.

[4] CBS News. "U.S. investigating if Iran was behind cyberattack on water systems in 7 states, including Minnesota and Michigan." CBS News, 2026.

[5] Jeffrey Burt. "More than 100 water systems were hit in July cyberattacks." The Register, August 26, 2026.

[6] James Reddick. "Cyberattacks on water systems expand to 12 states as South Dakota, Georgia anno unce incidents." The Record from Recorded Future News, August 5, 2026.

[7] Cybersecurity and Infrastructure Security Agency. "Iranian-Affiliated Cyber Actors Exploit Programm able Logic Controllers Across US Critical Infrastructure." CISA, April 7, 2026.

[8] CISA. "CISA, FBI, EPA and U.S. Government Partners Update Warning of Iran-Affiliated Threat Actors Targeting Critical Infrastructure Programmable Logic Controllers." CISA, July 22, 2026.

[9] Tenable Research. "CyberAv3ngers: FAQ About Iran-Linked Threat Group Targeting U.S. Critical Infra structure." Tenable, 2026.

