ISSUE BRIEF

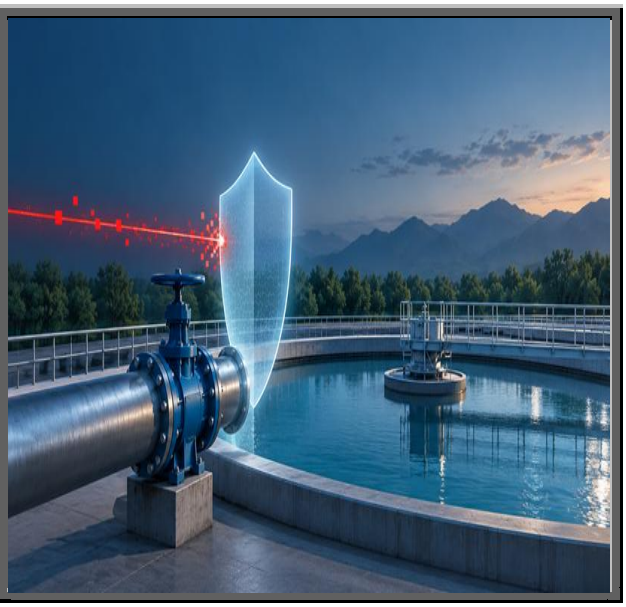
INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

POLAND'S WATER TREATMENT CYBERATTACKS: LESSONS FOR PAKISTAN'S CRITICAL INFRASTRUCTURE

By
Samar Khalid
Intern
Centre for Strategic Perspectives (CSP), ISSI
Email Address: csp@issi.org.pk

Supervised by
Muhammad Taimur Fahad Khan

September 14, 2026



Poland's Internal Security Agency (ABW) published its 2024–2025 activity report in May 2026. It recorded more than 40,000 reports of potential information and communication technology (ICT) incidents during the two-year period and documented unauthorised access to water-treatment control systems in Jabłonna Lacka, Szczytno, Małdyty, Tolkmicko, and Sierakowo.[1] Attackers altered equipment parameters, creating a risk to the continuity of local water supplies. Although the Polish and Pakistani contexts differ, the underlying weaknesses, poor credential security, and internet-exposed industrial-control interfaces are not country-specific and could plausibly exist in Pakistan's critical infrastructure. The Polish case therefore offers relevant lessons for prevention and preparedness.

The Global Rise of Attacks on Water and Power Infrastructure

Water and power utilities are attractive targets because they deliver essential services and disruptions produce immediate public consequences. The Polish water-treatment breaches were part of a broader pattern. On December 29, 2025, attackers targeted more than 30 wind and solar farms, a manufacturing company, and two combined heat-and-power plants.[2] At one facility, a destructive

[1] Internal Security Agency (ABW), *Polish Internal Security Agency (ABW) 2024–2025: Selected Activities*, Warsaw, 2026, pp. 36–38. https://www.abw.gov.pl/download/25/4876/ABWreport20242025.pdf

[2] CERT Polska, "Incident Report: Energy Sector, December 2025," January 2026.

wiper attack was blocked before causing damage; another facility, disclosed in a CERT Polska follow-up report in August 2026, was compromised through a misconfigured private cellular network and experienced a brief outage.[3] ESET linked elements of the campaign to Sandworm, a Russia-linked group, with medium confidence.[4] Together, these incidents demonstrate sustained targeting of Poland's energy and water infrastructure.

These incidents form part of a wider pattern of pressure on Polish critical infrastructure. Deputy Prime Minister and Digital Affairs Minister Krzysztof Gawkowski stated that Poland was facing approximately 2,000–4,000 cyberattacks daily, with about 170,000 incidents recorded in the first three quarters of 2025.[5] A significant share was attributed by Polish authorities to Russian state-linked actors. Poland's decision to raise its 2026 cybersecurity budget to €1 billion reflects the scale and persistence of the threat and the priority attached to infrastructure protection.[6]

The Polish Water Treatment Breach

Attackers gained unauthorised access to the industrial-control systems of five Polish water-treatment plants. This was not merely a data breach: they altered technical parameters governing plant equipment, creating a direct risk to the continuity of water-supply operations, as documented by the ABW.[7]

The simplicity of the intrusion makes the case particularly instructive. The attackers reportedly relied on weak credentials and management interfaces exposed to the public internet rather than sophisticated malware or zero-day exploits. No advanced tooling was required; access was obtained through inadequately secured control panels.[8]

---

https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

3 CERT Polska, "Follow-Up Report of the December 2025 Energy Sector Incident," August 2026. https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/

4 ESET Research, "Russian Sandworm Group Attacks Energy Company in Poland with DynoWiper," January 2026. https://www.eset.com/us/about/newsroom/research/eset-research-russian-sandwormapt-attacks-energy-company-poland-with-dynowiper/

5 Barbara Erling, "Poland Says Cyberattacks on Critical Infrastructure Rising, Blames Russia," *Reuters*, October 10, 2025. https://www.reuters.com/technology/poland-says-cyberattacks-critical-infrastructure-rising-blames-russia-2025-10-10/

6 CERT-EU, "Cyber Brief 25-10," September 2025. https://cert.eu/publications/threat-intelligence/cb25-10/

7 Internal Security Agency (ABW), *Polish Internal Security Agency (ABW) 2024–2025: Selected Activities*, Warsaw, 2026, pp. 36–38. https://www.abw.gov.pl/download/25/4876/ABWreport20242025.pdf

8 Internal Security Agency (ABW), *Polish Internal Security Agency (ABW) 2024–2025: Selected Activities*, Warsaw, 2026, pp. 36-38.

The disclosure carries additional institutional significance. The ABW had not issued a comparable public account of its activities since 2014, suggesting heightened concern over the current threat environment. It did not attribute the water-treatment breaches to a specific state or group, although the wider report highlighted hostile activity associated with Russian intelligence services.

These incidents affected small-town water systems rather than major utilities in Warsaw or other large cities. This raises a broader policy question: how can smaller essential-service providers implement proportionate cybersecurity controls? Limited scale does not make such facilities less exposed to attack.

A Common Weak Point

The comparison does not assume that an attack in Poland will be replicated in Pakistan. The two countries face different geopolitical circumstances and threat actors. Rather, the relevant vulnerabilities such as weak credentials and internet-exposed industrial-control systems, are structural and not country-specific. It is therefore plausible, though not confirmed, that similar weaknesses could exist in Pakistan's critical infrastructure. Pakistan can draw lessons from Poland without assuming identical vulnerabilities or threat scenarios.

Pakistan's power sector faces documented governance, oversight, and monitoring shortcomings across government-owned distribution companies.[9] These conditions do not establish the presence of the specific vulnerabilities exploited in Poland, but they reinforce the need to verify whether basic cybersecurity controls are implemented consistently. Water services are administered through provincial and municipal bodies, including Water and Sanitation Agencies and Tehsil Municipal Authorities.[10] This decentralised structure may complicate consistent implementation and oversight, although publicly available evidence on individual utilities' cybersecurity budgets and staffing remains limited.

Zscaler ThreatLabz identified a malicious file on NEPRA's public website in 2022 and linked it to SideWinder through shared infrastructure. The finding may indicate a website-level compromise, but it does not establish access to NEPRA's internal network or operational systems. It nevertheless

https://www.abw.gov.pl/download/25/4876/ABWreport20242025.pdf

9 National Electric Power Regulatory Authority, *State of the Industry Report 2025*, Islamabad, January 16, 2026. https://nepra.org.pk/publications/State%20of%20Industry%20Reports/State%20of%20Industry%20Report%202025.pdf

10 Asian Development Bank, *Water and Other Urban Infrastructure and Services Sector Assessment*, Manila, 2023. https://www.adb.org/sites/default/files/linked-documents/55236-001-ssa.pdf

demonstrates that entities associated with Pakistan's power sector have attracted state-linked espionage activity.[11]

No comparable compromise of Pakistan's operational-technology systems has been publicly confirmed. The possible website-level incident involving NEPRA does not demonstrate access to the grid, but it underscores the value of active monitoring and verification rather than assuming that the absence of public disclosure indicates the absence of risk.

The Preparedness Gap

Pakistan's primary gap is not the absence of rules but uneven implementation and enforcement. The Pakistan Information Security Framework (PISF), approved by the cabinet in 2026, requires network segregation, continuous monitoring, and tested backup and recovery procedures with defined recovery-time objectives.[12] It also requires controlled remote connectivity through measures including VPNs, monitoring, and auditing, while identifying multifactor authentication as a preferred rather than mandatory safeguard.[13] These controls address the types of weakness exposed by the Polish case. The CERT Rules 2023 provide the institutional basis for sectoral CERTs, including in the power sector, although operational establishment remains in progress.[14] In mid-2026, PKCERT's Director General stated that regulators such as NEPRA were still developing the relevant capabilities.[15] What remains unclear is the extent to which these requirements have been implemented and independently audited at individual power and water utilities, particularly at provincial and municipal levels.

Pakistan already has a functioning National CERT under the CERT Rules 2023[16] and holds full

11 Zscaler ThreatLabz, "WarHawk: New APT Backdoor from SideWinder," October 2022. https://www.zscaler.com/blogs/security-research/warhawk-new-backdoor-arsenal-sidewinder-apt-group

12 National CERT/NTISB, *Pakistan Information Security Framework (PISF) 2026: Essential System and Communication Protection Controls*, Sections B, D, and E, Government of Pakistan. https://pkcert.gov.pk/uploads/2026/03/Essential-System-and-Communication-Protection-Controls.pdf

13 National CERT/NTISB, *Pakistan Information Security Framework (PISF) 2026: Essential System and Communication Protection Controls*, Section B, paragraph 4(d), Government of Pakistan. https://pkcert.gov.pk/uploads/2026/03/Essential-System-and-Communication-Protection-Controls.pdf

14 Government of Pakistan, *Cyber Emergency Response Teams (CERTs) Rules, 2023*, Gazette of Pakistan, October 3, 2023. https://pkcert.gov.pk/uploads/2023/10/GAZETTE-CERT-Rules-2023.pdf

15 "Cyber Defence: Public, Private Entities Told to Set Up 'SOCs' in 6 Months," *Business Recorder*, July 2, 2026. https://www.brecorder.com/news/amp/40428085

16 Government of Pakistan, *Cyber Emergency Response Teams (CERTs) Rules, 2023*, Gazette of Pakistan, October 3, 2023. https://pkcert.gov.pk/uploads/2023/10/GAZETTE-CERT-Rules-2023.pdf

membership in FIRST[17] and operational membership in APCERT.[18] The remaining challenge is to strengthen sector-specific coordination for power and water, build dedicated operational-technology expertise, and ensure that enforcement reaches individual utility operators rather than stopping at the national level.

Poland's experience demonstrates the value of a well-resourced institution capable of investigating and publicly disclosing infrastructure-level breaches. Publicly available reporting does not yet demonstrate comparable utility-level investigation and disclosure capacity in Pakistan, particularly across smaller provincial and municipal operators.

Policy Recommendations

1. NEPRA should commission independent, regulator-supervised audits of power utilities' compliance with PISF requirements for network segregation, remote access, and monitoring. Provincial local-government departments, WASAs, and Tehsil Municipal Authorities should establish equivalent audit arrangements for water utilities. Both tracks should include time-bound remediation deadlines for identified deficiencies.
2. PKCERT and NEPRA should develop and enforce OT-specific cybersecurity standards for the power sector. For the water sector, PKCERT should work with provincial local-government departments, WASAs, and relevant municipal authorities to issue equivalent guidance suited to industrial-control environments.
3. NEPRA's planned sectoral CERT should provide specialist OT-security training for power-sector personnel and verify backup and recovery requirements through periodic incident-response exercises. Provincial water authorities should establish corresponding training, backup-testing, and exercise programmes for water utilities.
4. PKCERT should ensure that threat intelligence obtained through FIRST and APCERT reaches power and water utilities through their respective regulatory and sectoral channels, supported by regular joint incident-response exercises.

Conclusion

The Polish breaches show how weak credentials and internet-exposed control interfaces can place essential services and public safety at risk. Pakistan has made tangible institutional progress through

[17] FIRST, "Member Teams," accessed August 2026. https://www.first.org/members/teams/

[18] APCERT, "Member Teams," accessed August 2026. https://www.apcert.org/about/structure/members.html

the National CERT, membership in FIRST and APCERT, and the PISF 2026 framework. The remaining priority is to set firm implementation deadlines, verify compliance independently, and enforce cybersecurity controls at the utility level. Addressing these gaps before a comparable incident occurs would be considerably less costly than responding after operational disruption..