SHIELDWORKZ

IRAN-LINKED OT THREAT UPDATE

FOR WATER AND ENERGY OPERATORS

HOW TO READ THIS ADVISORY 3

EXECUTIVE INTELLIGENCE SUMMARY 5

- Key Findings 5
- Threat Outlook 6
- Sectors at high risk 6
- Immediate actions recommended 6

SITUATION OVERVIEW 8

- Geopolitical context 8
- Cyber activity associated with the conflict 8
- Historical precedent: Iran's use of cyber operations against critical infrastructure 9
- Strategic context: Why critical infrastructure, and why now? 9

CALIFORNIA WATER INCIDENT ANALYSIS 11

- What Happened 11
- What is confirmed 11
- What remains unknown 11
- OT systems potentially affected 12
- Exposure pathways involved 12
- Operational implications 12
- Critical assessment: Incident classification 13

INTELLIGENCE ASSESSMENT: IRANIAN OT TRADECRAFT 15

- Objectives 15
- Common tactics 15
- Target selection patterns 16
- Scenario 1 — Opportunistic targeting 18
- Scenario 2 — Coordinated critical infrastructure campaign 18
- Scenario 3 — Strategic retaliatory operations 19
- Scenario 4 — Influence and psychological effects operations 20

EXPOSURE ANALYSIS FOR WATER AND ENERGY OPERATORS 21

- Internet-exposed OT assets 21
- GNSS Dependency Risk 21

REGIONAL EXPOSURE ASSESSMENT 24

- North America 24
- GCC region 24

INTELLIGENCE-LED EXPOSURE SCAN RECOMMENDATION 27

- Internet-exposed OT exposure assessment 27
- GNSS dependency exposure assessment 27
- Executive Deliverables 28

STRATEGIC INSIGHTS 29

- What most organizations are missing 29
- Dangerous assumptions 29
- Why Internet-exposed OT assets remain common 29
- When geopolitical risk transforms into operational risk 30
- What boards and executives should be discussing 30

IMMEDIATE DEFENSIVE ACTIONS 31

- Next 24 Hours 31
- Next 7 Days 31
- Next 30 Days 32

ABOUT THIS ADVISORY 33

SHIELDWORKZ.....33

Strategic context: The California Water Service intrusion claim in strategic and operational context — with implications for North American and Gulf Cooperation Council critical infrastructure operators

Advisory Reference: SWZ-CTI-2026-019

Publication Date: 24 June 2026

Distribution: Unrestricted

Sectors: Water and Wastewater · Electric Power · Oil & Gas · Desalination · Transportation · Manufacturing

Prepared by the Shieldworkz OT Threat Intelligence Team
shieldworkz.com

HOW TO READ THIS ADVISORY

This advisory follows a structured intelligence-writing convention so that readers can quickly distinguish what is established from what is interpreted. Four categories of statement appear throughout:

Confirmed Fact	A claim independently verified by the affected organization, a government authority, or multiple reputable technical sources (e.g., Cal Water acknowledging an investigation; CISA publishing indicators of compromise).
Reported Claim	A statement made by a threat actor, victim, or single media source that has not been independently corroborated. Reported claims are attributed to their source and should not be read as fact.
Intelligence Assessment	A judgment made by a named threat intelligence provider (e.g., Dataminr, Unit 42, Gambit Security) based on technical analysis, expressed with its own confidence level.

Analyst Judgment	Shieldworkz's own interpretation, synthesis, or forecast, clearly labeled as such and assigned a confidence level using the scale below.

Confidence levels in this advisory follow standard intelligence community convention:

- **High confidence:** Judgment is based on high-quality, corroborated information from multiple independent sources, or direct technical evidence.
- **Moderate confidence:** Information is credibly sourced and plausible but not independently corroborated, or is corroborated but not fully consistent.
- **Low confidence:** Information is fragmentary, single-sourced, of uncertain reliability, or the analytic argument is one of several plausible alternatives.

Where this advisory references Shieldworkz's own prior research (the H1 2026 OT Threat Advisory, regional regulatory playbooks, and remediation guides), it does so to provide continuity of analysis, not as independent corroboration of the events discussed here.

EXECUTIVE INTELLIGENCE SUMMARY

On 11–12 June 2026, the Iran-linked persona Handala (publicly attributed by the U.S. Department of Justice to Iran's Ministry of Intelligence and Security, operating as Void Manticore) claimed a cyber intrusion against California Water Service (Cal Water), the largest investor-owned water utility in the western United States, naming its Bakersfield, Visalia, and Chico districts. The claim was explicitly framed as retaliation for U.S. strikes two days earlier on reservoirs near Sirik, Iran. Independent technical analysis and Cal Water's own preliminary findings indicate the confirmed access was limited to a customer billing database and an RTKBase GNSS correction server — an IT-side exposure, not an operational technology (OT) compromise. This advisory uses that incident as a case study to examine the wider pattern of Iran-linked targeting of water and energy infrastructure across North America and the Gulf Cooperation Council (GCC) during the 2026 Iran war and its fragile ceasefire.

Key Findings

- The Cal Water incident is best assessed, with **moderate-to-high confidence**, as a **strategic-signaling and psychological-operations event** rather than evidence of an OT disruption capability. No water production, treatment, or distribution system compromise has been confirmed by Cal Water, CISA, or independent researchers.
- The incident is not isolated. It follows a confirmed, government-attributed campaign: the 7 April 2026 joint CISA/FBI/NSA/EPA/DOE advisory (AA26-097A) documents Iranian-affiliated actors causing **real operational disruption** — HMI/SCADA data manipulation, configuration wiping, and sensor tampering — at U.S. water, energy, and municipal facilities via internet-exposed Rockwell Automation/Allen-Bradley PLCs.
- Iran-linked actors operate a deniable proxy model: hacktivist-branded personas (Handala/Void Manticore, Ababil of Minab) are used as a public-facing cover for MOIS and IRGC-linked units, confirmed forensically in the case of the March 2026 LA Metro breach (attributed to MOIS by Gambit Security) and officially by the U.S. Department of Justice in the case of Handala.
- GNSS dependency is an underappreciated exposure pathway. The same Cal Water incident involved an RTKBase GNSS correction platform, while the broader conflict has produced sustained, operationally consequential GPS jamming and spoofing across the Strait of Hormuz and Persian Gulf, disrupting over 1,100 vessels in a single 24-hour period at the height of the conflict. The mechanisms are directly relevant to timing-dependent OT environments on land.
- GCC water and energy infrastructure carries structurally higher humanitarian and strategic stakes than equivalent North American assets: the region depends on desalination for the large majority of its drinking water, and desalination, transmission, and oil & gas nodes have already been directly struck or disrupted during the conflict.

- The 17 June 2026 Islamabad Memorandum of Understanding extended the U.S.–Iran ceasefire by 60 days but resolved none of the underlying drivers (nuclear file, sanctions, Hormuz access, Lebanon front). Cyber operations against critical infrastructure are assessed, with **moderate confidence**, to continue at an elevated tempo through the ceasefire window regardless of kinetic status.

Threat Outlook

Shieldworkz assesses, with moderate confidence, that Iran-linked targeting of Western and GCC water and energy infrastructure will persist through at least the current 60-day ceasefire window (to mid-August 2026), driven less by the state of the kinetic conflict than by the proxy ecosystem's own operational momentum and the political utility of infrastructure-themed claims, whether or not they are technically substantiated. A renewed kinetic escalation — plausible given the fragility of the Lebanon front and unresolved Hormuz access dispute — would likely produce a corresponding spike in both genuine OT-targeting activity (in the CyberAv3ngers/Shahid Kaveh Group tradition) and psychological-operations claims (in the Handala tradition). Operators should not calibrate their posture to the apparent technical sophistication of any single claim; the April 2026 CISA advisory demonstrates that some of this activity does reach OT and produces real disruption.

Sectors at high risk

Sector	Risk Level	Primary Vector Observed
Water & Wastewater (NAM)	**Critical**	Internet-exposed PLCs/HMIs; billing-IT/OT boundary; vendor remote access
Desalination & Water Authorities (GCC)	**Critical**	Physical strikes on co-located power; cyber recon of SCADA; humanitarian leverage
Electric Power & Transmission	**High**	PLC exploitation; GNSS timing dependency for grid synchronization
Oil & Gas (NAM & GCC)	**High**	Drone/cyber convergence; export-terminal and processing-hub targeting
Municipal / Transport Operators	**High**	IT-to-OT pivot from virtualization and rail-control display systems (LA Metro)
Critical Manufacturing	**Moderate**	Supply-chain and IT-disruption spillover (Stryker precedent)

Immediate actions recommended

- Verify that no PLC, HMI, or OT-adjacent gateway (including GNSS reference stations, telemetry concentrators, or remote terminal units) is reachable from the public internet; prioritize Rockwell Automation/Allen-Bradley and Unitronics devices given confirmed Iranian targeting.
- Treat GNSS-derived timing and positioning data as advisory, not authoritative, in any OT process where precise time synchronization, asset geolocation, or telemetry timestamping affects safety or billing integrity.

- Audit segmentation between customer-facing IT systems (billing, CRM, GNSS correction platforms) and OT networks; the Cal Water pattern shows attackers reaching GNSS/billing infrastructure first and probing for lateral movement from there.
- Re-validate incident response and crisis-communications plans against a scenario where a threat actor publicly claims OT access before technical investigation can confirm or refute it — the reputational and stakeholder-confidence risk is immediate even when the technical risk is not.
- GCC operators specifically: confirm continuity plans for desalination-dependent water supply assume potential co-located power disruption, not only direct cyberattack, given the conflict's demonstrated pattern of hitting power infrastructure that feeds desalination.

SITUATION OVERVIEW

Geopolitical context

The current threat activity sits inside the 2026 Iran war, a conflict that opened on 28 February 2026 when the United States and Israel launched coordinated strikes (Operation Epic Fury (U.S.) and Operation Roaring Lion (Israel)) against Iranian military, nuclear, and leadership targets, including the killing of Supreme Leader Ali Khamenei. Iran retaliated with missile and drone strikes against Israel, U.S. regional bases, and Gulf states, and disrupted maritime traffic through the Strait of Hormuz, through which roughly 20 percent of global oil and gas exports transit.

A first ceasefire took effect on 8 April 2026 after nearly six weeks of fighting, but the underlying disputes relating to Iran's nuclear program, sanctions relief, frozen-asset repatriation, free passage through Hormuz, and the status of the parallel Israel–Hezbollah front in Lebanon — remained unresolved, and low-intensity exchanges continued. On 17 June 2026, U.S. President Trump and Iranian President Pezeshkian signed the Islamabad Memorandum of Understanding, extending the ceasefire for a further 60 days to allow negotiation of a permanent settlement and reopening the Strait of Hormuz to commercial traffic. As of this advisory's publication, the arrangement remains fragile: Israel–Hezbollah fighting has continued intermittently despite a parallel ceasefire, and on 21 June 2026 President Trump issued a public warning against any renewed Iranian attempt to close the Strait.

Analyst judgment (moderate confidence): the ceasefire's structural fragility (particularly the unresolved Lebanon front and the absence of a final nuclear settlement at the time of publishing) means cyber operations against Western and GCC infrastructure should be read as an ongoing feature of the conflict's current phase, not a wartime anomaly that ends when kinetic operations pause. Iran-linked actors have consistently used cyber and information operations to maintain pressure and demonstrate reach during periods when direct military action is constrained by ceasefire terms.

Cyber activity associated with the conflict

Cyber activity escalated within hours of the 28 February strikes. Iran reportedly stood up a coordinating 'Electronic Operations Room' the same day, and threat intelligence providers tracked a surge to an estimated 60 or more hacktivist-branded groups active in support of Iran by early March, alongside pro-Russian collectives. When Iran's domestic internet was almost entirely disconnected for 47 days (a near-complete outage that began at the war's outset), state-aligned operators assessed with high confidence by Unit 42 to be based inside the country shifted to satellite connectivity, including Starlink-class VSAT services, to sustain operational tempo illustrating both the regime's intent to preserve offensive cyber capability through infrastructure disruption and the limits of internet shutdowns as a containment measure.

The conflict has also produced direct kinetic effects on digital infrastructure relevant to OT operators: drone strikes damaged cloud-provider facilities in the UAE and Bahrain in early March 2026, disrupting cloud and IT services including, briefly, customer access to banking platforms across the Gulf. This is a stark reminder that 'cyber risk' in this conflict is not confined to network intrusion; physical attacks on shared digital infrastructure (data centers, satellite ground stations, telecommunications) can produce the same operational consequences for OT-dependent organizations as a direct cyberattack.

Historical precedent: Iran's use of cyber operations against critical infrastructure

Iran-affiliated actors have targeted Western OT environments for over a decade, and the current campaign should be read as an intensification of an established pattern rather than a new phenomenon:

- **2013:** Iranian hackers accessed control systems of a small dam near New York City, with minimal operational impact, but establishing an early demonstration of intent against U.S. civil infrastructure.
- **November 2023 – 2024:** The IRGC Cyber Electronic Command-affiliated group publicly known as CyberAv3ngers (also tracked as Shahid Kaveh Group, Hydro Kitten, Storm-0784, Bauxite, and several other aliases) compromised at least 75 internet-exposed Unitronics PLC/HMI devices across U.S. water and wastewater systems and other sectors, defacing HMI displays with anti-Israel messaging during the Gaza war.
- **March–April 2026:** A related but distinct Iranian-affiliated cluster (tracked by Unit 42 as CL-STA-1128) shifted targeting toward Rockwell Automation equipment, reportedly staging FactoryTalk software on rented VPS infrastructure to support exploitation — a deliberate broadening beyond the Unitronics device class previously targeted.

Shieldworkz analyst judgment (high confidence): the persistence and evolution of Iranian PLC-targeting tradecraft across three separate escalation periods (2013, 2023–24, 2026) indicates a standing institutional capability and intent, not opportunistic or improvised activity. The shift from Unitronics to Rockwell devices in 2026 suggests deliberate capability expansion in response to defensive hardening of the previously favored device class.

Strategic context: Why critical infrastructure, and why now?

Cyber operations against water and energy infrastructure serve Iran's broader strategic position in at least three distinct ways, which are not mutually exclusive and frequently operate together (and overlap) within a single claimed incident:

- **Asymmetric retaliation.** Iran's conventional military capacity has been degraded by U.S. and Israeli strikes; cyber and information operations against civilian-facing infrastructure offer a comparatively low-cost, deniable means of demonstrating continued reach against the U.S. homeland and allied states.

- **Psychological and information effect.** Infrastructure framed as 'life-sustaining' water above all carries disproportionate psychological weight relative to its actual technical compromise. The Handala model of claim-first, amplify-via-state-media, technical-verification-later is optimized for this effect rather than for engineering disruption.
- **Plausible deniability via proxy branding.** Both Handala (DOJ-confirmed MOIS front, operating as Void Manticore) and Ababil of Minab (forensically attributed to MOIS by Israeli firm Gambit Security following the LA Metro breach) follow a consistent pattern. A invented hacktivist identity that is aggressively projected, ideologically coded messaging, and infrastructure that traces back to known Iranian state operations once investigated.

This pattern matters directly for how operators and the public should interpret claims like the Cal Water incident: the absence of confirmed OT compromise does not mean the activity is inconsequential, because the intended effect may be reputational, psychological, or reconnaissance-oriented rather than disruptive in the first instance.

CALIFORNIA WATER INCIDENT ANALYSIS

What Happened

On 11 June 2026, the Iran-linked persona Handala posted a claim on its blog asserting that it had compromised California Water Service (Cal Water), one of the largest investor-owned water utilities in the United States, serving roughly two million customers across approximately 100 California communities. The group published what it described as a 5GB proof-of-concept data dump and named three Cal Water districts (Bakersfield, Visalia, and Chico) as affected. Screenshots circulated by Handala through known and validated social media accounts and amplified via Iranian state outlet Press TV appeared to show customer billing records and internal dashboard interfaces.

Handala framed the operation explicitly as retaliation: two days earlier, on 10 June 2026, U.S. strikes reportedly damaged two water reservoirs near Sirik on Iran's Strait of Hormuz coast, with Iranian officials and local sources stating that more than 20,000 residents lost access to safe drinking water during a heat wave. Handala's own messaging drew the parallel directly — "strike Iran's water, hit California's water back" — and the group stated it had deliberately chosen not to disrupt water service, describing the operation as a warning rather than a disruption.

What is confirmed

- Cal Water confirmed that a claim of this nature was made on 11 June 2026 and stated publicly that it activated its cybersecurity response plan and is investigating in coordination with state and federal partners.
- Cal Water's preliminary internal scans, communicated through multiple statements between 12 and 16 June, found **no evidence of operational disruption** to its IT, OT, water production, water delivery, or billing-platform systems.
- Independent analysis by the threat-intelligence firm Dataminr — cited consistently across SecurityWeek, Manufacturing Business Technology, and regional outlets — assessed that the threat actor most likely accessed Cal Water's **RTKBase instance**, a GNSS base-station platform used for high-precision positioning, and from there moved laterally to a customer billing system. Cal Water's Chico district as a confirmed affected account based on transaction and account-record artifacts in the leaked data.
- No technical Indicators of Compromise (malware hashes, network artifacts) had been published by Handala or independent researchers as of this advisory's publication, which constrains independent verification of the claimed scope.

What remains unknown

- The true extent of network access achieved, including whether any reconnaissance or staging occurred beyond the RTKBase and billing systems identified by Dataminr.

- Whether the claimed 5GB figure accurately reflects data exfiltrated, or — consistent with Handala/Void Manticore's documented pattern of inflating or recycling prior data in other operations — overstates the actual scope.
- Whether Handala's stated 'ability to disrupt water access' reflects genuine technical capability that was deliberately not exercised, or is purely rhetorical, given that no OT-side access has been independently confirmed.
- Final, government-attributed confirmation of the intrusion's scope: at the time of writing, CISA and the FBI have not issued an incident-specific advisory on the Cal Water claim, distinct from the broader April 2026 advisory on Iranian PLC targeting (addressed below).

OT systems potentially affected

Based on all currently available reporting, no OT system (SCADA, PLC, pump control, treatment-process control, or distribution control) has been confirmed as accessed or affected. The confirmed and assessed access (billing database, RTKBase GNSS correction platform) sits on the IT side of Cal Water's environment. This distinction is consequential: it is the basis for Cal Water's continued operational statements and for the independent assessment that water delivery was never genuinely at risk in this specific incident.

Exposure pathways involved

The RTKBase GNSS correction platform is a noteworthy exposure pathway precisely because it sits structurally between IT and OT. RTKBase-class systems provide real-time kinematic correction data used for survey-grade positioning — relevant to asset mapping, infrastructure geolocation, and increasingly to autonomous or semi-autonomous field operations in utility environments. It is not itself a control system, but it is infrastructure-adjacent, often managed with less rigorous access control than core OT assets, and — as this incident demonstrates — can provide a foothold from which an attacker can pivot toward customer or billing systems that share network segments or credentials.

Analyst judgment (moderate confidence): the choice of an RTKBase/GNSS platform as an entry point, whether deliberate or opportunistic, is significant beyond this single incident. It indicates that GNSS-adjacent infrastructure is a discoverable and exploitable category of asset in the water sector that does not receive the same security attention as conventional PLCs and HMIs, despite sitting close to the OT boundary. This theme is developed further in the GNSS Dependency Risk section below.

Operational implications

To date, the operational impact has been reputational and privacy-related rather than physical: potential exposure of customer billing data (names, addresses, account numbers, payment history) creates fraud and phishing risk for affected residents, and the public claim itself has generated political attention (a California congressman publicly called the incident a 'wake-up call' and stated he was in contact with the

Department of Homeland Security). No regulatory or law-enforcement advisory specific to this incident had been issued as of publication.

Critical assessment: Incident classification

The required analytical question is whether this incident represents opportunistic targeting, strategic signaling, psychological operations, infrastructure reconnaissance, or genuine disruption capability. The evidence supports a layered assessment rather than a single category:

Opportunistic targeting	Partially supported. Water utilities are chronically under-resourced and present a broad, discoverable attack surface; an RTKBase instance left accessible is consistent with opportunistic discovery rather than a pre-selected, high-value target.
Strategic signaling	Strongly supported. The explicit, immediate retaliation framing tied to the Sirik reservoir strikes, and the deliberate two-day timing, indicate the operation was conceived and timed as a message, not merely as an opportunistic data-theft event.
Psychological operations	Strongly supported. Amplification via Iranian state media, the stated (unverifiable) claim of restraint ("we could have disrupted water but chose not to"), and consistency with Handala/Void Manticore's documented hack-and-leak, claim-amplify playbook all point to an information-effect objective as the primary driver.
Infrastructure reconnaissance	Plausible but unconfirmed. Access to a GNSS correction platform could support future asset-geolocation or timing-disruption reconnaissance; no evidence currently confirms this was the operational intent rather than an incidental pivot point.
Actual disruption capability	Not supported by current evidence. No OT access has been confirmed by any party, including Cal Water itself. Claims of an ability to disrupt water service should be treated as unverified threat-actor assertion, consistent with Handala's historical pattern of overstating impact for psychological effect.

Bottom-line analyst judgment (moderate-to-high confidence): the Cal Water incident is best characterized as a strategic-signaling and psychological-operations event with a secondary, lower-confidence reconnaissance dimension, layered on top of a genuinely opportunistic initial access vector. It is not, on current evidence, a demonstrated OT disruption event. Operators should resist both extremes of interpretation — dismissing the incident as inconsequential because OT was not reached, and treating Handala's disruption claims as established capability — and

instead use it as a concrete illustration of how IT-side, GNSS-adjacent infrastructure functions as an underexamined pathway toward the OT boundary.

INTELLIGENCE ASSESSMENT: IRANIAN OT TRADECRAFT

This section synthesizes confirmed government advisories, attributed incidents, and named threat-intelligence assessments into a structured picture of how Iran-linked actors approach OT-relevant targets. It draws principally on the 7 April 2026 CISA/FBI/NSA/EPA/DOE/CNMF joint advisory (AA26-097A), the November 2023–2024 CyberAv3ngers campaign it builds on, and the forensically attributed LA Metro and Cal Water incidents.

Objectives

- **Disruption:** The April 2026 CISA advisory is explicit that the observed activity — exploitation of internet-facing Rockwell Automation/Allen-Bradley PLCs across water, energy, and government-facilities sectors — "resulted in operational disruption and financial loss," including configuration wiping, manipulation of data displayed on HMI and SCADA screens, and tampering with software-based mechanical sensor readings. This is a government-confirmed disruption objective, not a claimed one.
- **Intelligence collection / access persistence:** Unit 42's tracking of cluster CL-STA-1128 staging Rockwell FactoryTalk software on rented VPS infrastructure indicates deliberate capability-building and persistence rather than smash-and-grab opportunism; the CyberAv3ngers lineage has historically maintained access to compromised devices for extended periods between active disruption events.
- **Influence operations:** Handala/Void Manticore's consistent claim-then-amplify pattern (including using Iranian state media as a distribution channel for the Cal Water claim) demonstrates an information-warfare objective that functions independently of, and often in absence of, confirmed technical compromise.
- **Strategic signaling:** Operations timed within 24–72 hours of kinetic events (the Cal Water claim following the Sirik strikes by two days; Handala's healthcare-sector targeting in the days immediately preceding the 28 February kinetic opening) indicate cyber activity is being used deliberately as a synchronized component of the broader conflict, not as an independent campaign on its own timeline.
- **Access persistence via proxy branding:** The use of multiple parallel personas (Handala, Ababil of Minab, MOISIRAN, Homeland Justice, KarmaBelow) for what investigators assess to be the same small set of underlying MOIS/IRGC units allows continued operational tempo even when individual brands are disrupted — for example, the March 2026 FBI seizure of Handala-linked domains did not end the broader campaign, which continued under other persona names.

Common tactics

Tactic	Evidence base
Internet-exposed HMIs / PLCs	AA26-097A (Rockwell/Allen-Bradley, 2026); prior CyberAv3ngers campaign against 75+ Unitronics PLC/HMI devices (Nov 2023–2024)

Tactic	Evidence base
Weak / default remote access	Rockwell Automation's own guidance (SD1771, 2026) reiterating that customers disconnect devices from the internet and harden remote-access configurations
VPN exploitation	Pattern consistent with prior Iranian-affiliated activity targeting VPN appliances as initial access, referenced in Shieldworkz's H1 2026 OT Threat Advisory regarding BAUXITE/CyberAv3ngers TTPs
Credential abuse / lateral movement	Cal Water incident (RTKBase credentials reportedly used to reach billing system); LA Metro (VMware vCenter access used to reach broader internal environment)
Third-party / vendor and platform compromise	LA Metro breach reached a rail-yard management and train-control display system via initial access to virtualization infrastructure, illustrating pivot from administrative to operational-adjacent systems
ICS / asset reconnaissance	Use of internet-wide scanning to identify exposed Rockwell/Unitronics devices; Dataminr's GNSS/RTKBase-specific assessment in the Cal Water case
Living-off-the-land (LOTL)	Consistent with the dominant TTP identified across Iranian and broader nation-state OT campaigns in Shieldworkz's H1 2026 OT Threat Advisory

Target selection patterns

- **Water utilities:** Cal Water (claimed, IT-side); the broader water/wastewater sector named explicitly in AA26-097A; Sage Water Resources' Duchesne, Utah salt-water disposal facility (attacked in March 2026, remediated by mid-June).
- **Energy providers:** Named explicitly alongside water and government facilities in AA26-097A; Qatar's Ras Laffan LNG complex and Saudi Aramco's Ras Tanura refinery experienced kinetic (drone) disruption in the same period, illustrating the sector's status as a priority target set across both cyber and physical vectors.
- **Municipal infrastructure:** LA Metro (forensically attributed to MOIS); AA26-097A names "Government Services and Facilities (to include local municipalities)" as a targeted category alongside water and energy.
- **Oil & gas:** Targeted primarily through kinetic and drone-strike vectors during the conflict to date (Ras Tanura, Ras Laffan), with cyber targeting of the sector assessed as an ongoing, lower-visibility complement based on historical Iranian APT interest in energy-sector ICS.
- **Critical manufacturing:** The Stryker medical-device manufacturer breach (claimed by Handala, March 2026) demonstrates the proxy ecosystem's willingness to target manufacturing and healthcare-adjacent supply chains for disruptive effect, even outside the water/energy core focus of this advisory.

Shieldworkz analyst judgment (high confidence): target selection during the current conflict phase correlates closely with kinetic events and is not randomly distributed. Incidents cluster within days of strikes on Iranian territory or Iranian-linked assets, and the choice of sector (water, energy, municipal transit) consistently

favors targets with high public visibility and emotional resonance over targets offering greater technical disruption potential. This is consistent with an actor optimizing for psychological and political effect, with OT disruption (where it occurs, as in AA26-097A) functioning as an escalatory option held in reserve rather than the default mode of operation.

Threat scenario analysis

The following four scenarios are not mutually exclusive and may unfold sequentially or in parallel. They are constructed from the patterns observed across the Cal Water, LA Metro, AA26-097A, and GCC kinetic-targeting evidence reviewed above, and are intended to support planning rather than to predict a single outcome.

Scenario 1 — Opportunistic targeting

An Iran-aligned or sympathetic actor (state-directed or loosely affiliated hacktivist) discovers and exploits a poorly secured, internet-exposed asset — a GNSS correction server, an exposed PLC, a default-credential remote-access portal — without prior target selection, then retroactively frames the access as a deliberate, ideologically motivated operation. The Cal Water incident's likely entry point (an exposed RTKBase instance) is consistent with this pattern.

Likelihood	**High**
Impact	**Low to Moderate**
Trigger Conditions	Continuous; driven by routine internet-wide scanning rather than a specific political or military trigger. Volume increases during periods of heightened hacktivist mobilization (e.g., the post-28 February surge to 60+ active groups).
Expected Victim Profile	Under-resourced municipal utilities, smaller water districts, and any organization with unmanaged internet-facing OT-adjacent infrastructure, regardless of strategic significance.
OT Implications	Typically limited to IT-side or OT-adjacent systems (billing platforms, GNSS/telemetry servers) rather than core control systems, unless the exposed asset happens to be a PLC or HMI directly.
Detection Opportunities	External attack-surface monitoring (Shodan-class exposure scanning); anomalous authentication attempts against internet-facing management interfaces; unexpected outbound connections from GNSS/telemetry servers.

Scenario 2 — Coordinated critical infrastructure campaign

A more centrally directed, government-attributed campaign — exemplified by the activity described in CISA's AA26-097A advisory — targets a specific device class (Rockwell Automation/Allen-Bradley PLCs) across multiple organizations and sectors in a coordinated fashion, producing confirmed operational disruption (HMI/SCADA data manipulation, configuration wiping, sensor tampering).

Likelihood	**Moderate**

Impact	**High**
Trigger Conditions	Sustained or renewed kinetic escalation; deliberate capability demonstration timed to negotiation milestones; retaliation for a specific, attributable Western or Israeli action against Iranian infrastructure or personnel.
Expected Victim Profile	Mid-to-large water, wastewater, and energy utilities operating the targeted device classes with internet-facing exposure; government-facilities and municipal operators are explicitly named alongside them in the April 2026 advisory.
OT Implications	Direct: this scenario, per CISA's own findings, has already produced HMI/SCADA display manipulation, configuration wiping, and sensor-reading tampering — i.e., genuine OT-layer impact, not merely IT-adjacent exposure.
Detection Opportunities	Indicators of compromise published in AA26-097A; monitoring for the specific IP ranges and behavioral patterns described in the advisory; integrity monitoring on PLC project files and HMI configuration baselines.

Scenario 3 — Strategic retaliatory operations

A discrete, high-visibility operation explicitly timed and framed as retaliation for a specific kinetic event, prioritizing message clarity and timing over technical sophistication or actual disruption. The Cal Water claim, timed two days after the Sirik reservoir strikes, is the clearest current example; the LA Metro and Stryker incidents fit a similar, if less explicitly time-linked, pattern.

Likelihood	**Moderate to High**
Impact	**Moderate (technical) / High (political-economic)**
Trigger Conditions	Any U.S., Israeli, or allied kinetic action perceived by Iran as targeting civilian-facing infrastructure, water, or population centers; renewed strikes during the current ceasefire window would very likely trigger a comparable response within 24–72 hours.
Expected Victim Profile	High-symbolic-value, publicly recognizable operators — major utilities, transit authorities, or well-known consumer-facing companies — selected for the resonance of their name rather than the technical value of their networks.
OT Implications	Often limited to IT/data layers, but the operation's communicated framing may overstate or imply OT/disruption capability regardless of actual technical access, creating a gap between claimed and confirmed impact that operators must manage publicly.

Detection Opportunities	Monitoring of Iranian state media and Telegram channels associated with known MOIS-linked personas for claim activity; correlating claim timing against recent kinetic events; rapid internal forensic triage capability to confirm or refute claims before public narrative solidifies.

Scenario 4 — Influence and psychological effects operations

Operations designed primarily to generate fear, uncertainty, and erosion of public confidence in critical infrastructure security, independent of — and sometimes entirely without — actual technical compromise. This is Handala/Void Manticore's core documented operating model: claim, amplify via state media, allow ambiguity about technical access to do the work of generating concern.

Likelihood	**High**
Impact	**Low (technical) / Moderate-to-High (reputational and societal)**
Trigger Conditions	Ongoing, opportunistic, and largely decoupled from specific kinetic triggers; intensifies during periods of negotiation stress or when the regime seeks to demonstrate continued capability to domestic and international audiences.
Expected Victim Profile	Any organization whose name carries public recognition and whose sector (water, healthcare, transit) evokes immediate public concern, regardless of actual security posture.
OT Implications	Minimal to none in most cases; the objective is narrative and psychological rather than technical. However, repeated unverified claims create "crying wolf" risk that can blunt public and institutional response to a genuine future event.
Detection Opportunities	Media and dark-web monitoring for emerging claims; pre-established rapid-response communications protocols; partnership with sector-specific information-sharing bodies (e.g., WaterISAC, E-ISAC) to cross-check claim plausibility quickly.

EXPOSURE ANALYSIS FOR WATER AND ENERGY OPERATORS

Internet-exposed OT assets

The single most consistent thread across every confirmed and assessed incident in this advisory — the April 2026 CISA advisory, the historical CyberAv3ngers campaign, and the Cal Water RTKBase exposure — is that the initial access point was discoverable from the public internet. This is not a coincidence of attacker capability; it reflects a structural exposure problem across the sector.

- **HMIs and SCADA gateways:** Remain attractive because compromise produces immediately visible, photographable, shareable effect (a defaced HMI screen) that serves the influence-operations objective described above, in addition to any genuine control-layer access it provides.
- **Engineering workstations:** Represent a high-value pivot point because they typically hold credentials and project files (e.g., Rockwell FactoryTalk projects) for multiple downstream PLCs, converting a single compromise into broad device-level access.
- **Remote access infrastructure (VPNs, jump hosts, vendor portals):** Continues to be the most common initial-access category across nation-state OT campaigns generally; Rockwell Automation's own 2026 guidance reiterating that customers disconnect devices from the internet is a direct acknowledgment that this exposure remains widespread despite years of prior advisories.
- **Cellular-connected assets and telemetry systems:** Increasingly common in distributed water and energy infrastructure (remote pump stations, pipeline monitoring, distributed energy resources) and frequently deployed with carrier-default or weak authentication, since they are perceived as physically remote and therefore lower-risk — an assumption the GNSS/RTKBase pattern in the Cal Water incident directly contradicts.

Why these assets remain attractive: they are cheap to discover (via routine internet-wide scanning), often run with default or weak credentials, are infrequently patched due to operational-continuity concerns, and — critically for an actor with an influence-operations objective — their compromise is visually and narratively compelling even when the underlying technical access is limited.

GNSS Dependency Risk

The Cal Water incident's confirmed access to an RTKBase GNSS correction platform is not an isolated curiosity; it sits inside a much larger, currently demonstrated vulnerability in the GNSS ecosystem that the 2026 Iran war has stress-tested at unprecedented scale.

Since the conflict's 28 February opening, the Strait of Hormuz, Persian Gulf, and Gulf of Oman have experienced sustained GPS/GNSS jamming and spoofing, attributed by the U.S. Maritime Administration to a combination of Iranian electronic-warfare activity and defensive jamming by U.S. and allied forces. The operational consequences have been concrete and severe, not theoretical:

- More than 1,100 vessels experienced GPS and AIS interference in the Middle East Gulf within a single 24-hour period at the conflict's outset, with ships' navigation systems falsely reporting positions over airports, a nuclear power plant, and dry land.
- By early March 2026, the Joint Maritime Information Centre recorded over 600 individual GNSS disruption events in a single 24-hour window, and commercial transit through the Strait fell to near-zero on at least one day.
- Major war-risk insurers (Gard, Skuld, NorthStandard, the American Club) withdrew coverage for Gulf and Iranian waters, demonstrating that the financial and insurance sector treats GNSS-dependent navigation risk in this theater as material, not residual.
- Aviation has experienced parallel effects: at least 169 aircraft flying over the eastern Arabian Peninsula were affected by GPS spoofing on a single day in early March 2026.

Why this matters directly to land-based OT operators in water and energy: GNSS is not only a navigation technology. The Royal Institute of Navigation's January 2026 report on maritime GNSS interference notes that a modern vessel can carry over 20 distinct systems across seven categories that consume GNSS data or timing — fewer than half of which are directly involved in navigation. The same structural dependency exists onshore:

- **Time synchronization:** Many substation, grid-control, and SCADA-historian systems use GNSS-derived time (commonly via IEEE 1588 Precision Time Protocol or NTP referenced to GPS) for event sequencing, fault recording, and billing-interval accuracy. Spoofed or degraded timing can corrupt event logs and protection-relay coordination without any direct network intrusion.
- **Grid synchronization:** Phasor measurement units (PMUs) used for wide-area grid monitoring depend on precise GPS timing to synchronize measurements across geographically distributed substations; sustained timing errors degrade situational awareness exactly when grid operators most need it.
- **Pipeline operations:** Leak-detection and flow-balancing systems that correlate timestamped sensor data across long pipeline runs are similarly exposed to timing manipulation.
- **Water distribution:** As the Cal Water incident itself demonstrates, GNSS correction infrastructure (RTKBase-class systems) is now embedded directly in water-utility operations for asset geolocation and survey-grade positioning — and was the actual, confirmed point of compromise in this case.
- **Communications infrastructure:** Telecom base stations frequently use GPS for network timing synchronization; degraded GNSS can cascade into communications outages that compound, rather than merely accompany, an OT incident.

Analyst judgment (moderate confidence): the maritime GNSS crisis in the Gulf is best understood as a live demonstration of a vulnerability class — not a maritime-specific problem. North American and GCC OT operators with GNSS-dependent timing or positioning functions should assume that the same jamming and spoofing techniques demonstrated at sea are technically transferable to terrestrial targets, and that an actor with both the access (as shown in the Cal Water case) and the electronic-warfare capability (as shown in the Hormuz case) to affect GNSS-dependent infrastructure has now demonstrated both halves of that capability separately within the same conflict. Shieldworkz has not identified confirmed evidence that the two capabilities have been combined against a single OT target to date; this is presented as a forward-looking risk, not an observed event.

The distinction between jamming, spoofing, and timing manipulation matters operationally:

- **Jamming** denies GNSS signal outright, which most modern receivers can detect and alarm on, prompting fallback procedures.
- **Spoofing** provides a false but plausible signal, which receivers may accept as valid without alarming — the more operationally dangerous case, since downstream systems (AIS in the maritime case; potentially SCADA historians or PMUs onshore) treat the position or time data as authoritative.
- **Timing manipulation** is a subset of spoofing focused specifically on the time signal rather than position, and is the variant most relevant to grid synchronization, event-log integrity, and billing-interval systems in OT environments.

REGIONAL EXPOSURE ASSESSMENT

North America

North American water and energy operators face a pattern of exposure rooted in fragmentation, legacy technology, and chronic under-resourcing rather than concentrated strategic vulnerability of the kind seen in the GCC. The sector's scale works against it: the United States alone has tens of thousands of separate water and wastewater systems, the overwhelming majority of which are small municipal operations with limited dedicated cybersecurity staff.

- **Water utilities:** AA26-097A names water and wastewater systems explicitly as a targeted sector alongside energy and government facilities; Sage Water Resources' Duchesne, Utah facility was attacked and required remediation in the same window as the Cal Water claim, indicating the targeting is distributed across utility size and type, not concentrated only on large, recognizable operators.
- **Wastewater facilities:** Share the same PLC/HMI exposure profile as drinking-water systems and are explicitly within scope of the April 2026 advisory's named sector.
- **Municipal operators:** The LA Metro breach demonstrates that municipal transit, not only water and power, sits inside the same Iranian-linked targeting pattern, and that the consequences (1,400 servers requiring individual forensic clearance before being brought back online) can be operationally significant even without OT-specific impact.
- **Power utilities:** Named in AA26-097A; the PLC device class targeted (Rockwell Automation/Allen-Bradley) is in widespread use across North American power-sector control environments, and more than 3,000 such devices were reported as visible on the public internet at the time of the advisory's publication, according to Nozomi Networks.
- **Energy infrastructure:** Faces the same internet-exposed-device pattern as water, with the added regulatory dimension that Bulk Electric System assets fall under mandatory, audited NERC CIP requirements — meaning the exposures described in AA26-097A carry direct compliance, not only operational, consequences for in-scope entities.

Common exposure pattern across North America: a persistent gap between IT-side hygiene (which has generally improved following years of ransomware-driven investment) and OT/OT-adjacent hygiene, where billing platforms, GNSS correction services, and engineering workstations frequently sit on flatter, less segmented networks than core control systems — precisely the boundary the Cal Water incident exploited.

GCC region

The Gulf Cooperation Council states face a structurally different — and in several respects more acute — risk profile than North America, driven by geographic

proximity to the conflict, direct kinetic targeting of energy infrastructure, and an extreme dependence on a small number of concentrated, capital-intensive facilities for both water and energy.

- **Desalination facilities:** GCC states operate more than 400 desalination plants and account for roughly 40 percent of the world's desalinated water production. Dependence is extreme in places: desalination supplies approximately 90 percent of Kuwait's drinking water, 86 percent of Oman's, and 70 percent of Saudi Arabia's. Saudi Arabia's Jubail plant alone supplies more than 90 percent of Riyadh's drinking water through a roughly 500-kilometer pipeline system — a single point of catastrophic failure for a national capital's water supply, a vulnerability flagged in U.S. diplomatic assessments as far back as 2008.
- **Oil & gas operators:** Have already experienced direct kinetic disruption during the conflict: Iranian drone strikes forced QatarEnergy to halt production and declare force majeure at its Ras Laffan LNG complex in early March 2026, and debris from intercepted drones caused Saudi Aramco to shut down its Ras Tanura refinery. These are confirmed, reported events, not assessed risk.
- **Transmission operators:** Iran struck a power station in Fujairah, UAE that supports one of the region's largest desalination plants — a direct illustration of the water-energy interdependence that makes transmission infrastructure a de facto water-security target even when water facilities themselves are not directly struck.
- **Water authorities:** Both Iranian and Iranian state-media sources have accused the United States of striking a desalination plant on Qeshm Island in the Strait of Hormuz (March 2026); the claim has not been independently verified by Western sources but illustrates that desalination infrastructure is being actively contested in the conflict's narrative, not merely at theoretical risk.
- **Smart infrastructure deployments:** The Gulf's significant investment in cloud and AI infrastructure has already shown physical vulnerability: drone strikes damaged cloud-provider facilities in the UAE and Bahrain in early March 2026, briefly disrupting banking-customer access and illustrating that the region's digital-transformation investments are not yet uniformly covered by the same physical-defense posture as traditional energy and water assets.

Why the GCC region is strategically attractive to Iran during escalation: the calculus combines high humanitarian leverage (desalination dependency means even modest disruption translates quickly into population-level distress), concentrated critical nodes (a small number of large facilities, rather than thousands of small systems, means each successful operation carries outsized strategic value), and the region's proximity and political alignment with U.S. and Israeli interests, making GCC infrastructure a lower-escalation-risk substitute target relative to direct strikes on the U.S. or Israeli homeland.

Analyst judgment (high confidence): the GCC water-energy nexus — where desalination output is directly contingent on uninterrupted power supply —

represents the single most consequential infrastructure interdependency in this conflict theater. A cyberattack does not need to reach a desalination plant's control system directly to threaten water supply; disrupting the transmission or generation capacity that powers it achieves a comparable effect, and transmission/generation assets are, on current evidence, exposed to both kinetic and cyber targeting vectors simultaneously.

INTELLIGENCE-LED EXPOSURE SCAN RECOMMENDATION

The pattern documented throughout this advisory — initial access consistently achieved through discoverable, internet-facing, OT-adjacent infrastructure rather than sophisticated zero-day exploitation — means the highest-leverage defensive investment available to most water and energy operators today is not a new control technology, but an accurate, current picture of their own external exposure. Shieldworkz recommends a structured, intelligence-led risk exposure assessment built around the two exposure classes this advisory has identified as most consequential and least examined by conventional vulnerability management programs.

Internet-exposed OT exposure assessment

This engagement maps an operator's external attack surface the way an adversary discovers it — through internet-wide scanning, passive reconnaissance, and protocol fingerprinting — rather than relying on internal asset inventories that frequently understate true exposure.

- **Discoverable OT assets:** Identification of PLCs, HMIs, RTUs, and engineering workstations reachable from the public internet, prioritized against the specific device classes (Rockwell Automation/Allen-Bradley, Unitronics) confirmed as targeted in CISA's AA26-097A advisory and the 2023–24 CyberAv3ngers campaign.
- **Remote access exposure:** Assessment of VPN endpoints, jump hosts, and vendor remote-access portals for weak authentication, unpatched appliances, and absence of phishing-resistant MFA — the initial-access category most consistently cited across nation-state OT campaigns.
- **Publicly reachable interfaces:** Specific attention to the asset class highlighted by the Cal Water incident (GNSS correction servers, telemetry concentrators, billing-adjacent platforms) that sit near the IT/OT boundary and are frequently excluded from conventional OT asset inventories.
- **Third-party pathways:** Mapping of vendor, integrator, and managed-service-provider access into OT environments, reflecting the documented pattern (LA Metro, broader CISA guidance) of attackers reaching operational-adjacent systems via administrative or virtualization infrastructure rather than direct control-system exploitation.

GNSS dependency exposure assessment

A purpose-built assessment addressing the exposure class demonstrated concretely by the Cal Water incident and the Strait of Hormuz jamming/spoofing crisis and not typically covered by conventional OT security assessments.

- **Timing dependencies:** Inventory of systems relying on GNSS-derived time (protection relays, PMUs, SCADA historians, billing-interval systems) and assessment of fallback behavior if GNSS timing is degraded or spoofed rather than simply lost.

- **Synchronization weaknesses:** Evaluation of whether time-synchronization architecture can detect spoofed signals (anomalous but plausible time/position data) versus only outright signal loss — the operationally more dangerous failure mode demonstrated in the maritime AIS case.
- **Operational resilience gaps:** Assessment of whether terrestrial alternatives (eLoran-class terrestrial timing, inertial or cellular-signal-based positioning, hardened multi-constellation receivers) exist as fallback for GNSS-dependent operations, mirroring the "security by diversification" approaches now being explored for maritime navigation.
- **Single points of failure:** Identification of any GNSS correction or reference infrastructure — such as the RTKBase-class platform compromised at Cal Water — that, if degraded, spoofed, or compromised, would propagate errors into multiple downstream systems simultaneously.

Executive Deliverables

Deliverable	Purpose
Executive Risk Report	Board- and C-suite-level summary translating technical exposure findings into business, regulatory, and reputational risk language
Exposure Inventory	Authoritative, scan-validated inventory of internet-facing OT, OT-adjacent, and GNSS-dependent assets, replacing assumption-based internal inventories
Attack-Path Analysis	Mapped routes from discovered external exposure through to OT impact, modeled on the documented Cal Water (RTKBase → billing) and LA Metro (virtualization → rail control display) pivot patterns
Threat Mapping	Correlation of identified exposures against the specific Iran-linked tactics, device classes, and indicators documented in this advisory and CISA's AA26-097A
MITRE ATT&CK for ICS Alignment	Mapping of identified exposures and recommended controls to MITRE ATT&CK for ICS tactics and techniques, supporting consistent internal and regulatory communication
Prioritized Remediation Roadmap	Sequenced, resourced remediation plan distinguishing immediate (24-hour), near-term (7-day), and structural (30-day and beyond) actions

Shieldworkz's regulatory playbooks and remediation guides (available at shieldworkz.com/regulatory-playbooks and shieldworkz.com/remediation-guides) provide framework-specific follow-on guidance, including IEC 62443, NIST CSF, and NERC CIP remediation paths for North American operators, and NCA OTCC and Saudi Aramco SACS-210 alignment for GCC operators, for translating exposure-assessment findings into a defensible compliance posture.

STRATEGIC INSIGHTS

Beyond the specific incident and tactical detail covered above, several broader patterns deserve direct executive attention.

What most organizations are missing

Most water and energy operators continue to scope their OT security programs around the control-system core, PLCs, HMIs, SCADA servers, while treating IT-adjacent systems like billing platforms, GNSS correction services, and telemetry concentrators as outside that scope, owned by a different team, and governed by different (typically lighter) security standards. The Cal Water incident is the clearest possible illustration of why this boundary is no longer defensible: the actual point of compromise was precisely one of these IT-adjacent, OT-proximate systems, and the lateral movement path ran from there toward, not away from, the operational environment.

Dangerous assumptions

- **"We're too small to be a target."** The Sage Water Resources incident (a salt-water disposal facility in Duchesne, Utah) and the breadth of municipal targeting documented in AA26-097A both demonstrate that Iran-linked actors are targeting opportunistically across utility size, not exclusively pursuing marquee names.
- **"If it's not a PLC, it's not OT risk."** GNSS correction platforms, billing systems, and engineering workstations are not control systems, but they are demonstrated pivot points toward control systems and, in the case of GNSS, can corrupt OT-relevant data (time, position) without any network intrusion into the control system at all.
- **"A claimed attack with no confirmed OT access is a non-event."** As the Threat Scenario Analysis shows, psychological-effects operations are explicitly designed to generate reputational and stakeholder-confidence damage independent of technical impact; treating unconfirmed claims as non-events cedes the narrative and communications response to the threat actor by default.
- **"GNSS is a maritime and aviation problem."** The Strait of Hormuz crisis is a live demonstration of a vulnerability class that is mechanically identical onshore wherever GNSS-derived time or position feeds an OT process — the Cal Water RTKBase compromise shows the access vector already exists in the water sector specifically.

Why Internet-exposed OT assets remain common

This is not primarily a technology problem. It persists because of three compounding organizational realities across the sector: first, OT environments are frequently managed by operations and engineering teams whose primary performance metric is uptime, not security, creating structural reluctance to disconnect or restrict access to systems that "work"; second, asset inventories are commonly self-reported and out of date, meaning organizations frequently do not know their own external exposure until an external scan or an incident reveals it; and third, budget and staffing for OT

security at small and mid-sized utilities (the overwhelming majority of the water sector by count) remains structurally below the level required to maintain continuous exposure management, even where awareness of the risk exists.

When geopolitical risk transforms into operational risk

The translation mechanism is direct and, in this conflict, has already been demonstrated rather than theorized: a kinetic event (a strike on Iranian infrastructure) produces a retaliatory political decision (target U.S. or allied critical infrastructure), which is executed through a deniable proxy (Handala, Ababil of Minab) against a discoverable exposure (an internet-facing GNSS server, a Rockwell PLC), producing an operational and reputational consequence (a billing-data exposure claim, an HMI defacement, a multi-week server-by-server forensic recovery) regardless of whether the geopolitical trigger itself ever appears in an operator's own threat model. Operators who treat geopolitical risk monitoring as a function separate from OT exposure management will consistently be surprised by the timing, even when they are not surprised by the eventual target category.

What boards and executives should be discussing

- Whether the organization's incident-response and crisis-communications plans account for a scenario where a threat actor's public claim outpaces the organization's own forensic confirmation — as occurred at Cal Water — and what is communicated to customers, regulators, and media in the interim.
- Whether GNSS-dependent systems (timing, positioning, correction services) have been explicitly inventoried and assessed, given that this advisory documents the first confirmed instance of this asset class as an actual point of compromise in the water sector.
- Whether the organization's segmentation model treats billing, CRM, and telemetry/correction platforms as part of the OT-adjacent attack surface requiring equivalent governance, rather than as conventional IT systems governed solely by enterprise IT policy.
- For GCC operators specifically, whether business-continuity planning for water supply explicitly models co-located power disruption as a primary failure mode, given the conflict's demonstrated pattern of striking transmission and generation assets that feed desalination.
- Whether the organization has a standing relationship with sector ISACs (WaterISAC, E-ISAC) and government partners (CISA, EPA's water-sector cybersecurity technical-assistance program) sufficient to receive and act on advisories like AA26-097A within hours rather than weeks of publication.

IMMEDIATE DEFENSIVE ACTIONS

Recommendations are organized by time horizon and, within each, by whether the action is tactical (technical/operational team-executed), operational (process and coordination), or strategic (leadership and governance).

Next 24 Hours

Tactical

- Query firewall, VPN, and external-facing asset logs for connections to or from any GNSS correction/RTKBase-class platform, billing system, or telemetry concentrator that should not be internet-reachable.
- Run an external exposure check (internet-wide scan data, such as Shodan/Censys-class sources) against your own IP ranges for visible Rockwell Automation/Allen-Bradley and Unitronics PLCs and HMIs, per the device classes named in CISA's AA26-097A.
- Confirm MFA is enforced, and ideally phishing-resistant, on every remote-access path into OT or OT-adjacent environments, including vendor and third-party access.

Operational

- Brief the incident-response and communications teams on the Cal Water pattern specifically: a public threat-actor claim may precede internal forensic confirmation by days, and a holding statement should be pre-drafted.
- Confirm reporting channels to CISA (or the relevant national authority) and sector ISACs are current and tested.

Strategic

- Brief executive leadership that this advisory exists and that the organization's posture has been checked against its specific findings, particularly the GNSS/billing exposure pattern.

Next 7 Days

Tactical

- Review logs against the indicators of compromise and vulnerable-port guidance published in CISA's AA26-097A for any historical or current activity.
- Inventory and assess all GNSS-dependent systems (timing, positioning, correction services) for fallback behavior if GNSS signal is degraded or spoofed, not only lost outright.
- Harden or disconnect any PLC, HMI, or engineering workstation found exposed in the 24-hour scan; apply Rockwell Automation's SD1771 guidance where its devices are in use.
- Audit network segmentation between billing/CRM/telemetry platforms and core OT networks; treat shared credentials or flat routing between them as a finding requiring remediation, not an accepted convenience.

Operational

- Conduct a tabletop exercise modeling Scenario 3 (Strategic Retaliatory Operations) from this advisory — a public claim, ambiguous technical confirmation, and active media interest within the first 48 hours.
- Validate vendor and third-party remote-access pathways into OT environments, mirroring the LA Metro pattern of virtualization-platform compromise propagating into operational-adjacent systems.

Strategic

- Commission, or schedule, an Internet-Exposed OT Exposure Assessment and a GNSS Dependency Exposure Assessment as described in this advisory's recommendation section, prioritizing whichever asset class the 24-hour scan flagged as most exposed.
- GCC operators: confirm with the relevant transmission/generation provider that business-continuity assumptions for desalination-dependent water supply account for co-located power disruption.

Next 30 Days

Tactical

- Complete remediation of all internet-exposed OT and OT-adjacent assets identified in the prior two windows; re-scan to confirm closure.
- Implement integrity monitoring on PLC project files and HMI configuration baselines to detect the kind of data manipulation described in AA26-097A.

Operational

- Complete attack-path analysis from any newly discovered external exposure through to potential OT impact, modeled on the documented Cal Water and LA Metro pivot patterns.
- Map current exposures and controls against MITRE ATT&CK for ICS to support consistent internal reporting and regulatory communication.
- Formalize a standing relationship with sector ISACs and relevant government cybersecurity technical-assistance programs if not already in place.

Strategic

- Present an executive risk report to the board summarizing exposure-assessment findings, remediation status, and residual risk in business terms.
- Re-evaluate IT/OT governance boundaries explicitly to bring billing, CRM, GNSS correction, and telemetry platforms under equivalent security governance to core control systems.
- Build the current threat picture, including this advisory's findings, into the next scheduled board-level cybersecurity briefing rather than treating it as a one-time alert.

ABOUT THIS ADVISORY

This advisory was prepared by the Shieldworkz OT Threat Intelligence Team for water, wastewater, electricity, oil & gas, utilities, manufacturing, and critical infrastructure operators in North America and the Gulf Cooperation Council region. Shieldworkz provides OT/ICS cybersecurity intelligence, exposure assessment, and regulatory advisory services, including the Internet-Exposed OT Exposure Assessment and GNSS Dependency Exposure Assessment described in this advisory, and the OThello Assess platform for rapid, sub-24-hour OT security assessment.

Additional Shieldworkz resources relevant to this advisory:

- Regulatory Playbooks (IEC 62443, NIS2, NIST CSF, NERC CIP, ransomware response, tabletop exercise templates): shieldworkz.com/regulatory-playbooks
- Remediation Guides (IEC 62443-2-1, NERC CIP NDR, NIST SP 800-53, supply chain): shieldworkz.com/remediation-guides
- Threat Reports (State of OT Security, FrostyGoop analysis, APAC OT threat report): shieldworkz.com/reports)

SHIELDWORKZ

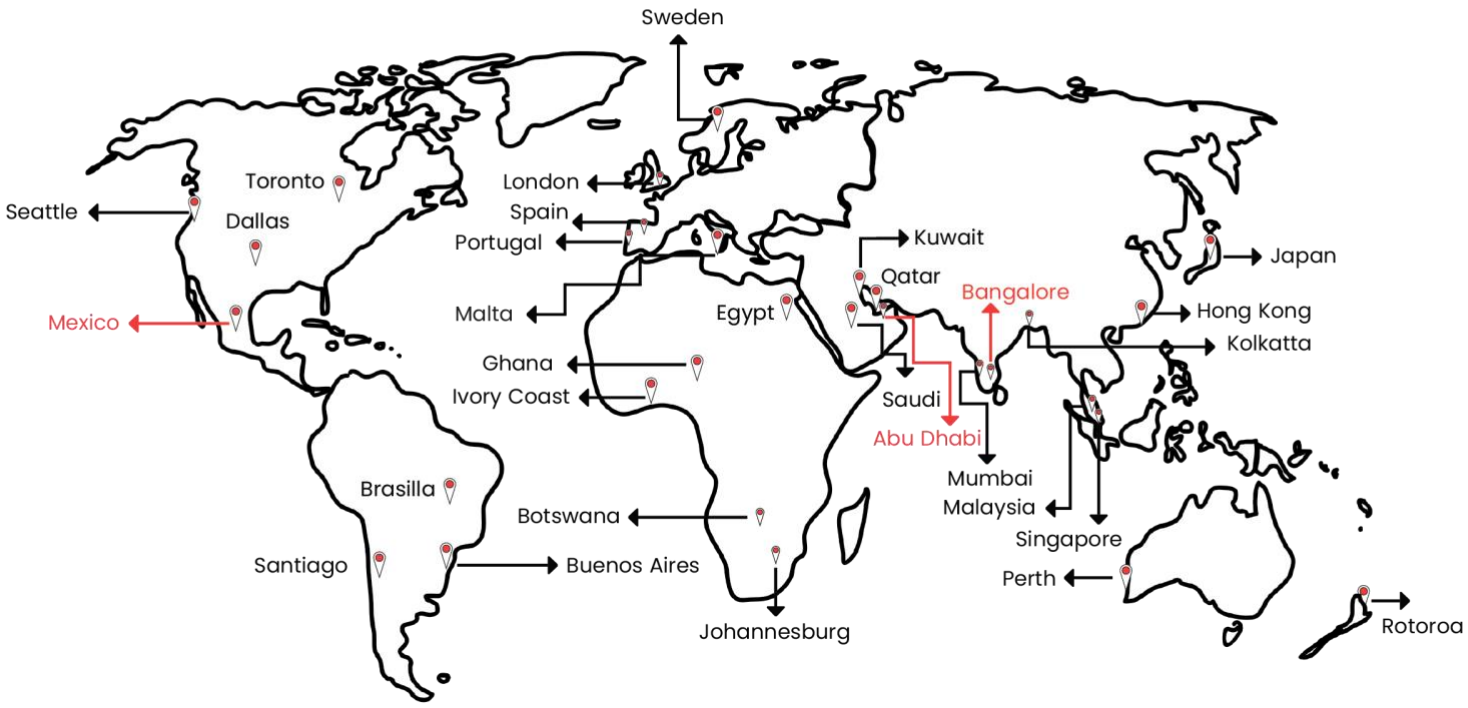
Shieldworkz is a specialist OT/ICS cybersecurity firm with an NDR solution and AI-based tools for securing SCADA, PLCs and Cyber Physical Systems. We serve critical infrastructure operators, industrial organisations, and government entities across the energy, oil and gas, manufacturing, utilities, transport, and defence sectors.

Our service areas include OT security assessments (powered by OThello Assess with sub-24-hour assessment cycles), NIS2 and IEC 62443 compliance programmes, OT threat intelligence advisories, OT SOC design and implementation, and regulatory readiness engagements for NCA (Saudi OTCC/ECC), NERC CIP, SOCI, and Singapore Cybersecurity Act obligations.

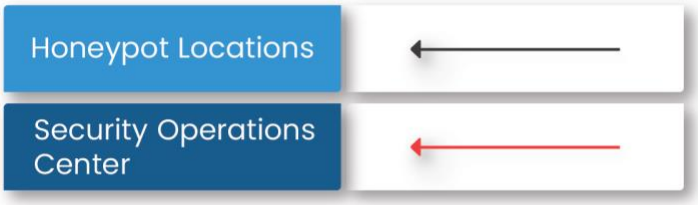
NDR Solution: shieldworkz.com/products/ot-security-platform **| Media Scan:** shieldworkz.com/products/ot-security- **| Othello Assess:** shieldworkz.com/othello/assess **| Patch Management:** shieldworkz.com/products/patch-management-solution **| Regulatory Playbooks:** shieldworkz.com/regulatory-playbooks **| Remediation Guides:** shieldworkz.com/remediation-guides **| Reports:** shieldworkz.com/reports

DISCLAIMER: This report is produced for informational and advisory purposes. Regulatory obligations vary by jurisdiction, entity classification, and operational context. This report does not constitute legal advice. Organisations should seek qualified legal and regulatory counsel to determine their specific compliance obligations.

About Shieldworkz



ISOC and Honeypot Locations



Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

SHIELDWORKZ

CONTACT US

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210
europe@shieldworkz.com

Tenth floor,
FAB BUSINESS CENTER

Abu Dhabi,
United Arab Emirates

+971 56 660 5200
middleeast@shieldworkz.com

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557
apac@shieldworkz.com