BESA
The Begin-Sadat Center
for Strategic Studies
Bar-Ilan University
PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

Iranian Cyber Sabotage Is Targeting US Water Systems

by Dr. Dany Shoham

BESA Center Perspectives Paper No. 2,405, August 25, 2026

EXECUTIVE SUMMARY: In a coordinated offensive, cyber actors directly linked to the Iranian regime recently executed a series of targeted digital intrusions against water infrastructure in the US. This aggressive campaign focused on the operational technology networks of municipal drinking water and wastewater treatment facilities across seven to twelve states. Unlike traditional cyber espionage campaigns, this unconventional and widespread operation was explicitly designed for real-world physical sabotage of a vital civilian resource.

Iran is actively engaged in cyber sabotage of water systems on the American homeland.

The primary mechanism of the attacks is the scanning of the public internet for exposed programmable logic controllers, which are the specialized industrial mini-computers responsible for managing physical machinery, water flow, and chemical treatment cycles. The attackers targeted facilities utilizing systems that were connected to the internet with vulnerable, factory-default administrative passwords. Upon gaining unauthorized access, the perpetrators aimed to immediately hijack the human-machine interface screens, alter administrative credentials, change system internet protocol addresses, and lock out local utility operators from their own digital control dashboards.

The targeted tampering apparently forced automation software offline, caused automated well systems to fail, and introduced immediate water pressure anomalies that triggered localized drops in supply. To reclaim ownership of

their infrastructure and protect public safety, municipal engineers would likely have had to sever their facilities from the internet and transition to emergency manual operations, relying on physical workarounds to keep water moving to their communities.

The attacked states included Minnesota, Michigan, Georgia, New Jersey, South Dakota, Utah, and Arkansas, among possible others.

The cascading risk to automated chlorination loops

A pivotal potential vulnerability exposed during this campaign was the indirect threat to the chemical treatment and safety of the supply of drinking water. While investigators found that the attackers had focused their direct inputs on mechanical infrastructure rather than manually adjusting chemical valves, the laws of fluid dynamics and water engineering mean that mechanical sabotage still destabilizes chemical composition.

Modern water purification relies on highly precise automated proportional dosing systems. These systems track the velocity and volume of water rushing through a plant and dynamically instruct chemical injectors to pump a perfectly balanced ratio of the disinfectant chlorine into the stream. By sabotaging the mechanical pumps and causing water velocity to fluctuate or halt completely, the hackers created a dangerous domino effect for the chlorination cycle. If water flow drops significantly at a particular location while automated chemical injectors continue to pump at pre-set levels, the concentration of chlorine in that section of the facility can rapidly skyrocket to toxic, highly corrosive levels. Conversely, the complete shutdown of pumping stations introduces the threat of water stagnation. Because chlorine is a volatile element that naturally degrades over time when standing still, prolonged stagnation in a town's disabled pipeline network causes the chlorination level to diminish or dissipate, paving the way for rapid, dangerous biological contamination due to inadequate disinfection.

Beyond imposing these threats, the perpetrators actively sought to alter programmable logic controller configuration parameters and thereby disable safety interlocks and automated shutdown commands. In a safely managed facility, these digital interlocks act as an automatic emergency brake: If a main water pump fails, the chemical pump instantly shuts off to prevent pure chemicals from pooling in a stagnant pipe. By attempting to rewrite this core logic and blind plant managers to ongoing system errors, the attackers intended to disable the safety measures designed to prevent harmful chemical

imbalances. In other words, an indirect disruption to the chlorination loop was a known, calculated outcome of the attackers' mechanical interference.

Official federal confirmations and industry warnings

The gravity of this threat to chemical processing was addressed in formal joint announcements released by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, and the Environmental Protection Agency. Federal defense units issued urgent public service announcements warning that state-sponsored threat actors were actively targeting the specific industrial control equipment used to adjust water quality, chemical treatment levels, and water pressure in US states. The Environmental Protection Agency noted that these types of breaches directly threaten a facility's ability to safely treat water or prevent the introduction of contaminants, highlighting how easily automated chemical loops can be desynchronized by remote interference like that conducted by Iran.

In technical threat assessments published specifically for infrastructure operators, national defense agencies identified the immediate cyber-physical risks facing the utility sector. Cybersecurity playbooks analyzing the exact hardware families compromised during the campaign formally warned that for the water sector specifically, a disrupted programmable logic controlling a chlorination loop can lead to toxic chemical overflows or water disinfection failures, threatening public safety at the municipal level. These field vulnerability disclosures confirmed that the threat actor's manipulation of configuration parameters posed a direct risk to water chlorination at municipal utilities, leaving systems entirely dependent on manual engineering workarounds to preserve basic chemical safety.

In explaining the sudden necessity for emergency monitoring, defense intelligence briefings connected the recent campaign to the past playbook of the identical state-sponsored threat groups. In previous international conflicts, specifically during a cyber operation deliberately targeting Israeli water infrastructure (see BESA Center Perspectives Paper No. 1,795, November 2, 2020, *The Quadruple Threat—North Korea, China, Pakistan, and Iran*), the adversary's primary objective was to poison the Israeli water supply by maliciously increasing the chlorine concentration. Because the putative attackers of the US water systems possess a documented history of targeting chlorination cycles, and because the same industrial control equipment targeted in the earlier operations against Israel is now under direct threat in the US, federal agencies are treating the recent American utility breaches with the highest level of national security urgency.

Classification as unconventional gray-zone warfare

Because of the strategic intent, the asymmetric nature of the targets, and the potential for cascading public health disasters, this overall sabotage event can be classified as a clear manifestation of unconventional gray-zone warfare. Gray-zone conflict represents aggressive operations executed by foreign states that take place above the line of ordinary peacetime competition yet below the threshold of open, declared military warfare. By utilizing digital agencies and deniable cyber tools rather than kinetic military strikes, the foreign adversary attempted to inflict severe physical and psychological damage on a domestic population while minimizing the risk of an immediate military counterattack.

While intelligence agencies are fairly confident that the campaign stemmed from Iran's Islamic Revolutionary Guard Corps (IRGC), investigators are still working to isolate the exact internal sub-unit. It remains unconfirmed as yet whether the attacks were executed directly by the IRGC Cyber Electronic Command, an affiliated proxy group like CyberAv3ngers, Handala (an IRGC/Ministry of Intelligence-linked group), or another branch, possibly one that is not yet recognized.

Irrespective of its actual impact, in the theater of unconventional conflict and weapons of mass destruction, this sabotage event borders, if indirectly, on the threshold of biochemical warfare insofar as it was a deliberate attempt to inflict a toxicant or contagion on an adversary population. The sabotage was designed to inject systemic panic into the US domestic homeland, drain public resources, and prove that a foreign adversary can silently compromise the safety of both US industry structures and individual Americans' household tap water from thousands of miles away. As Iran is accelerating development of the IRGC's Cyber Electronic Command and undoubtedly considering the operational adoption of other sabotage scenarios, heightened vigilance is essential.

Dr. Dany Shoham is a former senior analyst in IDF military intelligence and the Ministry of Defense. He specializes in chemical and biological warfare in the Middle East and worldwide.

BESA Center publications and research are made possible thanks to the generosity of Saul Koschitzky and family