TLP:CLEAR

Q3 2025

Water & Wastewater Sector

A Quarterly National Security Information-Sharing Bulletin from the U.S. Environmental Protection Agency and the Water Information Sharing and Analysis Center

In This Issue

Introduction—Drones/UAVs, Mediums For Physical Attacks In Relation To Chemical Security And The Interdependencies Of Critical Infrastructure

Unmanned Aerial Systems (UASs), commonly known as drones, have revolutionized the critical infrastructure community sector by enabling efficient and cost-effective inspections, reducing the need for manual labor and minimizing safety risks associated with hazardous environments. Additionally, they provide real-time data and high-resolution imagery, allowing for more accurate monitoring and maintenance of infrastructure assets, leading to improved operational efficiency and reduced downtime.

Nevertheless, drones can also pose significant threats to critical infrastructure, including power generation sites, chemical facilities, and water utilities, due to their accessibility, versatility, and potential for misuse. These threats can range from unauthorized surveillance, physical attacks, and even cyber attacks.

Drones equipped with high-resolution cameras or sensors can gather detailed information on sensitive infrastructure assets. Malicious actors could use this data to identify weak points for sabotage or other physical attacks. For example, drones could map security perimeters, monitor guard schedules, or detect unprotected access points. The risk of malicious actors using drones to attack a water utility's hazardous chemical supply is also a growing concern.

- In fact, in a recent incident reported to WaterISAC, a very large combined utility reported a significant burglary where multiple thieves broke into its water treatment plant and stole tens of thousands of dollar's worth of copper and other equipment. The utility reported that drones were spotted above the facility prior to the security breach, likely being used to facilitate the theft.

As seen during the Russia-Ukraine conflict, physical attacks using UASs present an ever-increasing risk. Drones can carry payloads like explosives or chemicals to damage facilities, equipment, or vehicles. Even small, commercially available drones can significantly disrupt operations by crashing into critical equipment, such as pumps or control systems. Commercially available drones can also be modified using 3D printed material to drop explosive devices or other material.

- In November 2024, for example, a domestic violent extremist reportedly planned to use a commercially available drone that he modified with explosives and fly it into an electric substation near Nashville. Law enforcement thwarted the plot before it could be executed.

Continues on page 2

“How To” Implement Basic Cyber Hygiene Actions—Basic/Practical “To-Dos”

Geopolitical tensions are increasingly reflected in the cyber domain, with nation state cyber actors from China, Russia, and Iran targeting U.S. critical infrastructure as a strategic tool to advance their interests and weaken American societal resilience. Recent government assessments and a growing number of articles highlight that critical infrastructure organizations such as water, energy, telecommunications, and transportation are now the prime target for these adversaries.

For example, China’s state sponsored groups have pre-positioned themselves within U.S. networks, as seen in campaigns like Volt Typhoon, ready to disrupt or destroy critical services during a crisis or conflict. Russian cyber actors, while avoiding direct military confrontation, conduct persistent cyberespionage and information operations to steal sensitive data and intellectual property. Meanwhile, Iranian linked groups have exploited vulnerabilities in water utilities and other sectors, sometimes in retaliation for U.S. foreign policy actions.

These incidents underscore a clear trend: sovereign sponsored and politically motivated cyberattacks are more frequent and sophisticated, posing heightened risks of infrastructure failure, economic disruption, and even loss of life. Cyber actors specifically seek out basic security weaknesses such as unpatched systems, default passwords, and insufficient employee training to gain initial access and maintain persistence.

To effectively counter evolving cyber threats, organizations must prioritize comprehensive cyber hygiene. Leading organizations such as the EPA, CISA, FBI, and WaterISAC recommend a set of foundational practices:

- Reduce Exposure to the Public-Facing Internet
- Conduct Regular Cybersecurity Assessments
- Change Default Passwords Immediately
- Conduct an Inventory of Operational Technology/Information Technology Assets
- Develop and Exercise Cybersecurity Incident Response and Recovery Plans
- Backup OT/IT Systems
- Reduce Exposure to Vulnerabilities
- Conduct Cybersecurity Awareness Training

These measures are critical, as cyber actors increasingly target gaps in basic security defenses. By consistently implementing these best practices, critical infrastructure operators can substantially reduce cyber risk and help ensure the protection of national security. 💧

If organizations require assistance or recommendations for implementing cyber hygiene best practices, please reach out to EPA and WaterISAC using the email listed below.

Read the full fact sheet here.

Additional Resources:

- EPA Cybersecurity for the Water Sector
- CISA - Water and Wastewater Cybersecurity
- WaterISAC - 12 Cybersecurity Fundamentals for Water and Wastewater Utilities
- AWWA - Cybersecurity Resources for Water Systems

Drones/UAVs *(continued from page 1)*

Mitigating these threats may require robust countermeasures like anti-drone-systems, enhanced surveillance efforts, restricted airspace designations, and employee training. To complicate matters, the world’s largest drone manufacturer, DJI decided in January this year to eliminate geofencing on its drones in the U.S., replacing automatic no-fly zone restrictions with optional enhanced warning zones. This raises concerns about the increased risk to critical infrastructure from potential unauthorized drone flights.

Critical infrastructure sectors, such as water and energy, are highly interdependent, where a disruption in one can cascade across others, amplifying impacts. In today’s dynamic threat environment, effective coordination and resilience planning across these sectors are essential to mitigate risks and ensure operational continuity.

Drones are now an aspect of everyday life, necessitating that critical infrastructure organizations plan to mitigate potential threats. 💧

Read more at CISA’s Be Air Aware program

Additional Reading:

- On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism
- Droning On: The Response to Use of Drones by Domestic Violent Extremists
- Are Domestic Drone Shoot-Downs Lawful?

Microsoft SharePoint Vulnerabilities Exploited by Chinese Threat Actors

On July 22, 2025, Microsoft shared information regarding the active exploitation of on-premises SharePoint servers that exploit CVE-2025-49706, a spoofing vulnerability, and CVE-2025-49704, a remote code execution vulnerability. These vulnerabilities affect on-premises SharePoint servers only and **do not affect SharePoint Online in Microsoft 365**. Microsoft has released new comprehensive security updates for all supported versions of SharePoint Server (Subscription Edition, 2019, and 2016) that protect customers against these new vulnerabilities.

Utilities that use Microsoft SharePoint Server on-premises are urged to fully review the guidance from CISA and Microsoft to address the high-severity vulnerabilities in SharePoint Server. This may require utilities that outsource technology support to **consult with their service providers for assistance with remediation actions.**

These comprehensive security updates address newly disclosed security vulnerabilities in CVE-2025-53770 that are related to the previously disclosed vulnerability CVE-2025-49704. The updates also address the security bypass vulnerability CVE-2025-53771 for the previously disclosed CVE-2025-49706.

The previously identified vulnerabilities, CVE-2025-49704 and CVE-2025-49706, commonly called “ToolShell,” can be exploited with public internet access unlike typical SharePoint exploits which require compromised credentials or other insider access. This significantly lowers the barrier for attackers, leading to increased attacks globally due to ease of exploitation. Threat actors leveraged these exploits to compromise hundreds of organizations across the globe.

Microsoft observed two named Chinese nation-state actors, Linen Typhoon and Violet Typhoon exploiting these vulnerabilities targeting internet-facing SharePoint servers. In addition, its analysts found another China-based threat actor, tracked as Storm-2603, exploiting these vulnerabilities to deploy ransomware.

Linen Typhoon and Violet Typhoon are Chinese-linked threat actors that have previously focused on intellectual property theft and espionage. They have historically targeted a variety of critical infrastructure sectors in the U.S., Europe, and East Asia. Microsoft also attributes Storm-2603 with medium confidence to Chinese threat actors.

Critically, given the rapid adoption of these exploits, *Microsoft assesses with high confidence that threat actors will continue to integrate them into their attacks against unpatched on-premises SharePoint systems, underscoring the importance of patching.* 💧

Additional Reading:

- Disrupting active exploitation of on-premises SharePoint vulnerabilities
- UPDATE: Microsoft Releases Guidance on Exploitation of SharePoint Vulnerabilities
- Customer guidance for SharePoint vulnerability CVE-2025-53770
- Active Exploitation of Microsoft SharePoint Vulnerabilities: Threat Brief (Updated July 31)
- CISA - People’s Republic of China Threat Overview and Advisories

U.S. Critical Infrastructure Organizations Encouraged to Heighten Vigilance for Potential Iranian Cyber Activity

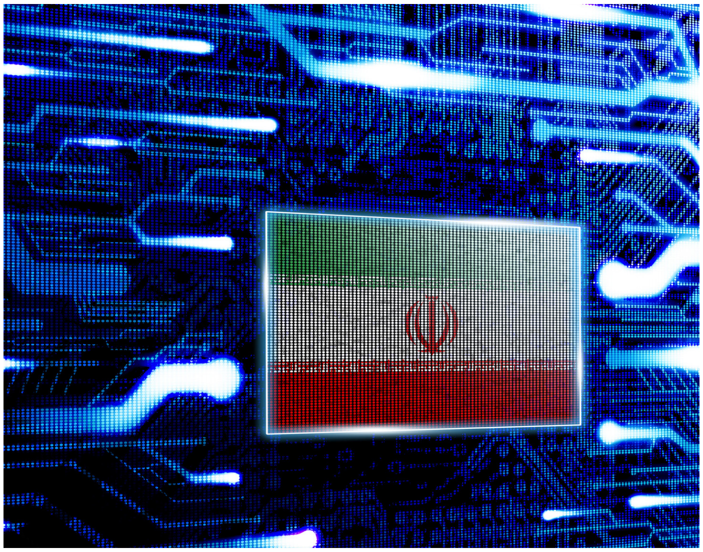
Following the U.S. strike on Iran's nuclear facilities in June, cybersecurity experts and government agencies are warning of a significant increase in the likelihood of retaliatory cyber attacks targeting U.S. critical infrastructure—including water and wastewater utilities. *Based on past periods of escalation, the conflict has the potential to pose a cybersecurity risk to U.S. citizens and organizations*.

Iran has a well-documented history of using cyber operations as an **asymmetric tool** in response to geopolitical tensions, such as sanctions or perceived acts of aggression. In the past, Iranian-linked threat actors have targeted critical infrastructure in retaliation of U.S. policy. In **November 2023**, for example, Iranian-affiliated actors operating under the Cyber Av3ngers persona gained unauthorized access to Israeli-made Unitronics Series ICS programmable logic controllers (PLCs) in multiple U.S. entities, mostly water and wastewater utilities, and defaced the PLCs' screens with an anti-Israel message. In response to the defacement, a few of the water-sector victims briefly shut down their systems and switched to manual operations. These attacks **continued** into 2024.

According to a recent U.S. government cybersecurity advisory, these actors often exploit targets of opportunity based on the use of unpatched or outdated software with known Common Vulnerabilities and Exposures (CVEs) or the use of default or common passwords on internet-connected accounts and devices. A successful intrusion could allow attackers to manipulate chemical dosing, disable pumps, or cause service outages, posing serious risks to public health and safety.

There is a **litany** of Iranian affiliated threat actors, including Islamic Revolutionary Guard Corps (IRGC)-affiliated advanced persistent threat (APT) cyber actors and aligned hacktivist groups. Among these actors, the CyberAv3ngers is a particularly noteworthy group given their past attacks against the water sector and their tactical adaptations. For instance, in December of 2024, it was revealed that the group had developed the **IOControl malware** to infiltrate industrial control systems and internet-of-things (IOT) devices globally.

Although, U.S. government agencies have not seen recent indications of a coordinated campaign of malicious cyber activity in the U.S. that can be attributed to Iran, the risk remains. Indeed, in past periods of escalation, Iran has **often waited** months or years to retaliate against its opponents in response to acts of aggression.



Ultimately, water and wastewater utilities, particularly smaller ones, are perceived as resource poor organizations that often lack robust cybersecurity defenses, making them attractive targets. Entities across the sector are encouraged to adopt basic cyber hygiene practices, such as network segmentation, multi-factor authentication, and regular patching. These steps will not only help reduce the risk of an attack by Iranian threat actors but also help enhance a utility's overall cybersecurity posture. 💧

For more information on Iranian state-sponsored threat actor activity, see CISA's ***Iran Cyber Threat Overview and Advisories*** *page.*

Additional Reading:

- **Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest**
- **Hardening US Infrastructure Before a Potential Iranian Cyber Attack**
- **Navigating Heightened Cyber Risks from Iranian Threats**

INSIDER THREAT – Former Employee Sentenced for Tampering with Utility’s Water Supply

Malicious insiders are an enduring reality for water and wastewater utilities. By way of an example, an incident occurred on the evening of November 29, 2022, involving an employee tampering with chlorine levels that could have caused serious public health impacts to the local community.

Incident: An employee of a water utility was found guilty of disabling the chlorination system used to disinfect the drinking water. The employee became **disgruntled** and **unhappy after being disciplined** and having his company truck taken away. In retaliation, the employee **used his trusted access** to enter the remote pumping station with a key and bypass the alarm with a code without immediate detection. The employee then proceeded to **use his knowledge** to shut off the chlorine pump. The employee also knew the importance of the chlorine pump in disinfecting water to provide safe drinking water to the public.

A letter from the town manager provided further details of the incident. According to the letter, an alarm monitoring chlorine levels would normally have been sent through the station’s remote monitoring system to the utility’s operational headquarters and to an on-call employee’s cellphone to alert them that the chlorine levels had fallen below a certain level. However, the alarm was also disabled.

The next morning, utility employees saw the chlorine pump had been shut off the previous evening and immediately restarted the chlorine pump. Employees “remained on site to verify it was functioning properly and chlorine levels were being restored,” the letter said. The utility responded in time to prevent chlorine levels from remaining low long enough to jeopardize water quality. After testing the water quality, it was determined that no additional action was necessary.

The town manager said afterwards it became apparent to utility employees the event was caused by “someone on the inside.” The entrance to the pumping station is blocked by a locked gate, a chain link fence surrounds the station’s building, and the door to the building itself is made of reinforced metal, but there were no signs of forced entry. Every employee “involved in water treatment functions had keys to this facility. Only someone with access to and knowledge of the alarm and chlorine systems could have adjusted them in this manner,” according to the town manager. This incident was investigated by local law enforcement and the Federal Bureau of Investigation.

Crime: Sabotage, the employee pleaded guilty to tampering with the drinking water supply.

Punishment: The individual was sentenced to a period of time-served (approximately one day) to be followed by three years of supervised release. The government recommended a sentence of one year and one day in prison.

**The charge for tampering with a water system provides a sentence of up to 20 years in prison, three years of supervised release and a fine of $250,000.*

Indicators: Disgruntlement.

Read more about Insider Threats at CISA here.

New National Terrorism Advisory System (NTAS) Bulletin and Security Risks Stemming from the Latest Middle East Conflict

On Saturday, June 21, the U.S. conducted strikes on Iranian nuclear facilities. Iran vowed retaliation. This has led to a heightened threat posture both domestically and internationally, as the Iranian regime could retaliate through multiple avenues. The next day, the Department of Homeland Security (DHS) issued a new National Terrorism Advisory System (NTAS) Bulletin to warn public safety officials of a significant escalation in the threat environment following recent U.S. actions in the ongoing conflict with Iran.

For water and wastewater operators maintaining situational awareness of geopolitical events overseas is critical because hostile nation states and their supporters can create security risks and operational impacts to critical infrastructure organizations in the U.S. homeland. In regard to hostilities in the Middle East, for instance, Iranian threat actors have previously targeted infrastructure in retaliation for U.S. policy.

Despite the announcement of ceasefire between Israel and Iran, federal officials are on high alert over potential threats in the homeland stemming from the conflict in the Middle East. Importantly, as Iran suffers continued military setbacks, it could seek to retaliate using asymmetrical means such as international terrorism, as it has done previously.

According to the NTAS, the escalation in the Middle East has led to a heightened threat environment in the U.S. homeland. The most immediate risk is the potential for low-level cyber attacks against U.S. networks by pro-Iranian hacktivists and cyber actors affiliated with the Iranian government (highlighted in a previous article). Iran also has a long-standing commitment to target the U.S. Government officials it views as responsible for the death of an Iranian military commander killed in January 2020.

Iran reportedly sent a message to President Trump in the days before the U.S. strikes threatening to activate "sleeper cells" inside the U.S. if it were attacked. Despite the lower probability of a domestic terrorist attack emanating from a "sleeper cell," the FBI director, Kash Patel, dedicated more resources to monitoring the possibility of "sleeper cells" linked to Iran and its terrorist proxies, such as Hezbollah.

U.S. Department of Homeland Security
National Terrorism Advisory System
Bulletin
DHS.gov/advisories

There is also the potential for violent extremists in the homeland to independently mobilize to violence in response to the conflict. Potential targets could include organizations perceived to be Jewish, pro-Israel, or linked to the U.S. government or military in the homeland. Violent extremists and other threat actors have previously conflated utilities and their personnel as extensions of the U.S. government, potentially increasing the risk to critical infrastructure.

Moreover, German authorities recently arrested an alleged spy working on behalf of Iran, who authorities say was collecting information on potential targets, underscoring the risk of targeted attacks in Western countries.

Multiple recent homeland terrorist attacks have been motivated by anti-Semitic or anti-Israel sentiment, and ongoing tensions between Israel and Iran could contribute to U.S.-based individuals plotting additional attacks. The ongoing Israel-Hamas conflict has already been the primary motivation of a number of recent extremist targeted attacks. It has also inspired physical attacks against critical infrastructure. 💧

Read the full NTAS here.

Securing Hazardous Chemicals Through CISA's Chemlock Security Program

Chemicals are vital to the economy and are used by organizations in many industries. However, in the hands of a violent extremist or an adversary with criminal intentions, some dangerous chemicals could be weaponized to harm a facility, its workers, or the surrounding community. Water and wastewater utilities often have significant quantities of hazardous chemicals at their facilities, making the protection of these elements a critical priority.

By considering the potential avenues of attack and approaching security holistically, facility owners and operators can choose cost-effective, efficient security measures that work best to protect their dangerous chemicals from the threats and hazards most likely to occur at their facility. Threats to facilities with hazardous chemicals can include, but are not limited to, physical attacks, insider threats, cyber attacks, unauthorized drone activity, power loss, and natural hazards such as powerful storms.

CISA's ChemLock program offers no-cost services and tools that can help utilities better understand the risks they face and improve their chemical security posture in a cost-effective manner. The tools and services offered by ChemLock include:

- **ChemLock On-Site Assessment and Assistance (OAA)**: A holistic chemical security assessment that helps you identify the security risks your on-site chemicals present; offers scalable, tailored suggestions for security measures; and assists you in developing a facility security plan customized to your facility.
- **ChemLock Resources**: Publicly available guidance documents, templates, fact sheets, and flyers to help facilities enhance the cyber and physical security surrounding your chemicals.

CHEM LOCK

Know your chemicals.
Lock in your security posture.

- **ChemLock Exercises**: Either a facilitated, tailored tabletop exercise or a suite of CISA Tabletop Exercise Packages (CTEPs) that you can download and use as desired.
- **ChemLock Training**: Virtual and in-person training to assist you with understanding the threat and what security measures can be put into place to reduce the risk of dangerous chemicals from being weaponized.

Additionally, EPA as the Sector Risk Management Agency (SRMA) for the water sector offers a variety of tools and guidance documents to support water and wastewater utility preparedness and response. For example, EPA offers a series of water contamination response resources.

By leveraging EPA's and CISA's resources, water and wastewater utilities can enhance their security posture and help prevent hazardous chemical incidents by understanding the risks and developing a culture of security awareness.

Learn more about CISA's ChemLock Program here and access EPA's Resilience Resources here.

Useful Links and Contact Information

For feedback, comments or questions related to the content in this bulletin, please email Water-NSISB@epa.gov

WaterISAC

- Website | www.waterisac.org/
- Membership Information | www.waterisac.org/membership
- Incident Reporting Form | www.waterisac.org/report-incident
- 24 Hour Line | 866-H2O-ISAC

EPA

- Office of National Security | www.epa.gov/national-security
- Drinking Water and Wastewater Resilience Website | www.epa.gov/waterresilience
- Cybersecurity for the Water Sector | www.epa.gov/waterresilience/epa-cybersecurity-water-sector

Water Sector Coordinating Council

- American Water Works Association
- Association of Metropolitan Water Agencies
- National Association of Clean Water Agencies
- National Association of Water Companies
- National Rural Water Association
- Water Environment Federation
- WaterISAC
- Water Research Foundation