

# 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

- Rising Geopolitical Tensions and Weaponized Supply Chain Interdependence Creating New Operational Risks for Water and Wastewater Utilities
- Foundations for Operational Technology Cybersecurity: Asset Inventory Guidance for Owners and Operators
- Russian-Aligned Hacktivist Cyber Attack Case Study - January 2024
- Insider Threat - Terminated Utility Employee Reportedly Called in Bomb Threat to Former Workplace and Threatened to Poison the Water Supply
- Cyber Threat Actor Profile - "CyberAv3ngers" (also known as CyberAveng3rs, Cyber Avengers)
- Blended Threat - Anti-Government Extremist Group Claims Credit for Weather Radar Sabotage, Calls for Further Action
- Operational Resilience - Strengthen Your Supply Chain with EPA's Supply Chain Resilience Resources

## Rising Geopolitical Tensions and Weaponized Supply Chain Interdependence Creating New Operational Risks for Water and Wastewater Utilities

Interdependent economies are the hallmark of today's globalized world. This globalized world is held together by vast networks of supply chains, which are now being reshaped amid rising geopolitical tensions. As countries race to secure the supply chains, a major shift in the global economy is underway, one in which interdependence itself has become a central arena of geopolitical competition, according to the [Soufan Center](#). Supply chain interdependencies and potential supply chain shocks can impact a water and wastewater utility's ability to operate and also introduces additional risk of various types of supply chain compromises.

Among the adversarial nation states seeking to undermine the U.S. and its global partners, China represents the greatest long-term challenge. The U.S. Intelligence Community's [2025 "Annual Threat Assessment,"](#) noted that "China's dominance in key supply chains enables its use of economic coercion against countries that adopt policies Beijing opposes. Beijing is developing an institutionalized framework enabling more assertive and centrally controlled trade retaliation." Moreover, in a speech in April 2020, Chinese President Xi Jinping stated his intentions to increase global supply chain dependencies on China, with an aim of controlling key supply chains and being able to use those supply chain dependencies to threaten and cut off foreign countries during a crisis

China's dominance in these markets could pose a significant risk to U.S. critical infrastructure, including



water and wastewater utilities, if China is able to adeptly leverage its dominance for political or economic gain. China could exploit our interdependent supply chains to disrupt U.S. water and wastewater utilities by disrupting use and dependencies on critical materials, components, and technologies sourced from Chinese manufacturers. Many U.S. water and wastewater utilities rely on imported equipment, such as pumps, valves, sensors, and control systems used in water treatment processes.

During a crisis or heightened geopolitical tension, China could impose export restrictions, delay shipments,

*Continues on page 2*

or introduce subtle cybersecurity threats into Chinese-manufactured products, which could disrupt maintenance schedules, impair operational reliability, or compromise digital infrastructure. Such disruptions could cascade across the sector, affecting water quality, service continuity, and public confidence, particularly given the limited domestic manufacturing capacity and long replacement lead times for specialized parts.

In addition to potential disruptions of Chinese manufactured devices (this includes devices made in countries outside China, where the electronics inside the case are Chinese sourced), Chinese devices that are used by U.S. critical infrastructure organizations could be leveraged for espionage purposes or even to facilitate destructive cyber attacks. Chinese [security cameras](#) and [drones](#), for instance, are noteworthy concerns. U.S. critical infrastructure organizations use both kinds of devices extensively as part of their operations. Security cameras devices typically lack data encryption and security settings and have default settings to communicate with their manufacturer back in China. Similarly, Chinese drones have the ability to collect sensitive information, which could be relayed to China state-sponsored threat actors and exploited during future operations.

Additionally, in May 2025, undisclosed communication devices, including cellular radios, were [discovered](#) inside Chinese manufactured power inverters and batteries used in U.S. renewable energy infrastructure, such as solar and wind electric generation facilities. These devices “provide additional, undocumented communication channels that could allow firewalls to be circumvented remotely, with potentially catastrophic consequences,” a U.S. government official said.

This incident highlights the risk of [foreign components](#) in operational technology systems. The global supply chain for OT is a complex web, with components often sourced from multiple countries to optimize cost and efficiency. However, this efficiency is often to the detriment of security best practices. Foreign components with embedded backdoors or remote access capabilities could allow adversaries to

manipulate or disable critical systems, such as the Chinese-made cameras mentioned above. In addition to risk of foreign-made hardware, the China and other state-sponsored threat actors have [increasingly](#) targeted the software supply chain.

Another emerging dynamic is Chinese entities purchasing [land](#) and sensitive sites across the U.S., which could be used



to facilitate malicious activities. In New Hampshire, for instance, media reports noted that China’s largest beverage company recently [bought](#) a large commercial property near a local water utility. Although these actions are legal, they have the potential to create risk for utility operators since this Chinese company could gain unauthorized physical access to the local utility’s distribution network.

Going forward, geopolitical tensions are likely to continue growing, furthering the risk of hostile nation states weaponizing interdependent supply chains to generate operational disruptions in U.S. critical infrastructure entities. Therefore, maintaining awareness of the geopolitical landscape, understanding supply chain dependencies, and developing redundant suppliers can greatly help mitigate the risk of supply chain disruptions in today’s evolving threat landscape. 💧

#### Additional Reading:

- [Protecting Critical Supply Chains: A Guide to Securing Your Supply Chain Ecosystem](#)
- [Weaponized Interdependence: Supply Chains Reconfigure Globally](#)
- [Unseen Threats: The Hidden Risks of Foreign Components in Critical Infrastructure](#)
- [How Does Hybrid Warfare Impact the Global Supply Chain?](#)

# Foundations for Operational Technology Cybersecurity: Asset Inventory Guidance for Owners and Operators

In August, EPA, CISA, and other federal and international partners published a report, “Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators,” to help operational technology (OT) owners and operators across all critical infrastructure sectors create and maintain OT asset inventories and supplemental taxonomies.

An asset inventory is a regularly updated, structured list of an organization’s systems, hardware, and software. It includes a categorization system—a taxonomy—that classifies assets based on their importance and function. These tools help owners and operators identify which assets in their environment should be secured and protected, and structure their defenses accordingly to reduce the risk a cybersecurity incident poses to the organization’s operational capabilities.

The guidance outlines a process for OT owners and operators to create an asset inventory and OT taxonomy. This process includes defining scope and objectives for the inventory, identifying assets, collecting attributes, creating a taxonomy, managing data, and implementing asset life cycle management. The guidance details how OT owners and operators can maintain, improve, and use their asset inventory to protect their most vital assets. To help illustrate real world examples of OT taxonomies, CISA developed conceptual taxonomies through working sessions with organizations in the energy and water and wastewater sectors.

The first two controls in the [Center for Internet Security’s \(CIS\) Critical Security Controls](#) pertain to creating an inventory of assets. Fundamental 5 “Account for Critical Assets” from WaterISAC’s [12 Cybersecurity Fundamentals for Water and Wastewater Utilities](#) provides additional guidance, specifically for the water sector, to help utilities account for critical assets. In addition, [EPA’s Guidance for Improving Cybersecurity at Water and Wastewater Systems](#) and its [Cybersecurity Incident Action Checklist](#) include maintaining an updated asset inventory as a priority cybersecurity practice for water and wastewater



An asset inventory is a fundamental cybersecurity component of any organization’s security program. Water and wastewater utilities are encouraged to review the guidance to understand how to build and maintain OT asset inventories and implement the recommended actions. These practices can help utilities improve their cybersecurity posture and reduce the risk of compromise in operational environments. 💧

[Access the full guidance report here.](#)

## Additional Reading:

- [Principles of Operational Technology Cyber Security](#)
- [Fundamental 5 “Account for Critical Assets” | WaterISAC’s 12 Cybersecurity Fundamentals for Water and Wastewater Utilities](#)
- [Center for Internet Security’s \(CIS\) Critical Security Controls](#)
- [EPA’s Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems](#)

# Russian-Aligned Hacktivist Cyber Attack Case Study – January 2024

As the need for increased connectivity grows, coupled with aging infrastructure, critical infrastructure entities have become ideal targets for adversaries seeking to exploit organizations with poor cybersecurity practices. Adding to this is rising geopolitics tensions and an accompanied increase in cyber threat activity, which can culminate in high-profile attacks, such as the attacks on several water utilities in Texas in January 2024. This case study delves into the cyber threat activity that attempted to disrupt essential services, highlighting the attackers' tactics, the organization's response, and the lessons learned to fortify defenses against future incursions. Through an in-depth analysis, this open-source study aims to provide valuable insights into enhancing cybersecurity measures within the water and wastewater sector.

This cyber incident affected a couple of small utilities in Texas, in January 2024. Attackers associated with the Cyber Army of Russia Reborn (CARR) – a Russian-aligned hacktivist group – claimed to have infiltrated the industrial control systems of some local water towers and caused them to overflow. In response to this attack, one of the utilities swiftly transitioned to manually operating its water system, ensuring continued service to residents while mitigating the risk of further digital tampering. Meanwhile, the other neighboring utilities successfully thwarted the cyber actors' attempts to breach their systems. They promptly relayed this information to federal authorities, aiding in the broader investigation and contributing to efforts to identify and prosecute the threat actors responsible for the coordinated attack.

Upon further analysis based on open-source information and commercial resources into the cyber incident affecting the Texas utilities, water towers seem to suggest a common denominator: a third-party vendor's remote access software that was employed across the facilities. Publicly available information theorizes that the software potentially could have served as the avenue through which threat actors attempted to infiltrate and manipulate the water tower systems. Despite this vulnerability, the utilities' quick response ensured that essential services remained operational, minimizing the impact of the attack. While the overflow incident was undoubtedly an annoyance, the uninterrupted availability of water services underscored the resilience of the utilities' infrastructure. This incident sheds light on the importance of third-party risk management and the necessity of maintaining close relationships with all vendors, along with stringent software security to implement stricter access controls to prevent future breaches.



Following these intrusions, federal authorities initiated an investigation that led to the identification and sanctioning of two Russian nationals involved in orchestrating the cyber attacks. These sanctions represent a significant step in holding perpetrators accountable and serve as a warning to other potential cyber threat actors. By imposing these measures, the authorities not only seek justice for the affected communities but also aim to deter future attacks on critical infrastructure. This underscores the importance of international cooperation in combating cybercrime and reinforces the commitment to safeguarding essential public services from malicious actors.

## Helpful Takeaways

The following takeaways may be used by water utility owners to augment cybersecurity practices.

- Maintain healthy relationships with all their vendors and managed service providers, where all parties can contribute to a strong cybersecurity culture. This includes routine communication to mitigate any potential vulnerabilities identified from either party. Cybersecurity is a shared responsibility, and everyone plays a pivotal role in protecting their industrial environments from cyber threats.
- Consider using EPA's new [Cybersecurity Procurement Evaluation Checklist](#), which aims to help water and wastewater utilities assess the cybersecurity practices of vendors, manufacturers, and service providers.
- Implement best practices for remote services to Industrial Control Systems (ICS) and Operational

Technology (OT) environments to safeguard this critical infrastructure from cyber threats while ensuring operational efficiency and security. Some mitigations from the MITRE ATT&CK Framework on remote services techniques in ICS environments include:

- **Access Management:** Enforce authentication on critical remote services.
- **Authorization Enforcement:** Provide privileges corresponding to the restriction of a GUI session to control system operations.
- **Filter Network Traffic:** Filter application-layer protocol messages for remote services to block any unauthorized activity.
- **Human User Authentication:** Require strong authentication before providing user access for all remote services.
- **Network Allowlists:** Specify what external connections (e.g., IP address, MAC address, port, protocol) can be made from a device.
- **Network Segmentation:** Segment and control software movement between business and OT environments by way of one directional demilitarized zone (DMZs).
- **Password Policies:** Enforce strong password requirements.
- **Software Process & Device Authentication:** Authenticate all communication sessions to remote services to prevent unauthorized access.
- **User Account Management:** Limit the accounts that may use remote services. 💧

## Sources:

- U.S. Department of Treasury: [Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn](#)
- CISA: [Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity](#)
- CNN: [Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says](#)
- Lubbock Online: [Feds sanction Russian hackers who infiltrated Muleshoe, Abernathy municipal water systems](#)
- Gov Tech: [Overflowing Water Tank Linked to Russian Cyber Attack](#)
- [CrowdStrike](#)
- Intelligence Tipper: Pro-Russia Hacktivist Group Cyber Army of Russia Profile (CSIT-24194)
- [Mandiant](#)
- Cyber Physical Threat Actor Spotlight: [CyberArmyofRussia\\_Reborn \(24-10006168, Version: 2\)](#)
- Russia-Linked 'Hacktivist' Group Cyber Army of Russia Reborn Claims Manipulation of Texas Water Facilities' OT (24-00004451, Version: 2)
- [MITRE ATT&CK Framework](#)
- ICS Techniques: [Remote Services \(T0886\) Mitigations](#)

## **INSIDER THREAT – Terminated Utility Employee Reportedly Called in Bomb Threat to Former Workplace and Threatened to Poison the Water Supply**

Malicious insiders are a persistent threat to water and wastewater utilities. Disgruntled employees, in particular, can pose a significant threat to a utility's operations due to their unique insider knowledge. An incident from earlier this year demonstrates the operational disruptions a disgruntled employee can cause, highlighting the importance of implementing a rigorous insider threat management program.

**Incident:** In February of 2025, a former disgruntled utility employee was **arrested** for allegedly making a bomb threat at the utility and for threatening to poison the utility's water supply. The disgruntled employee's threats of violence caused significant operational disruptions to the utility. Prior to the incident, the employee had been terminated.

The former employee reportedly called in a bomb threat at the utility's water treatment plant and said he was going to "kill everyone," which caused an evacuation of the facility until K9 officers could clear the building. He also sent several threatening messages to employees in another administration building. That building was put under lock down out of safety for employees since the alleged perpetrator was a former employee and knew the facility. In a

voicemail, the former employee also threatened to "poison the water supply."

According to local media reports, the employee made multiple calls to other utility employees threatening acts of violence and using obscene language. The perpetrator reportedly made 44 unwanted calls to just one utility employee. Following the threats of violence, police were able to identify the former employee and subsequently arrest him.

**Crime:** Threat of violence. Three separate criminal dockets were filed against the former employee, who faces numerous charges including felony counts of terroristic threats that cause the evacuation of a building and terroristic threats that caused serious public inconvenience and misdemeanor counts of terroristic threats and harassment.

**Punishment:** At the time of this writing, the court case remains ongoing.

**Indicators:** Disgruntlement. The former employee was fired and was likely seeing retribution. 💧

[Read more about insider threats at CISA here.](#)

## **CYBER THREAT ACTOR PROFILE – “CyberAv3ngers” (also known as CyberAveng3rs, Cyber Avengers)**

### **Group Association**

Advanced Persistent Threat (APT) cyber group affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC).

### **Noteworthy Activity**

The CyberAv3ngers are infamously known for **compromising** and defacing Unitronics PLCs across several U.S.-based water and wastewater utilities, like the incident at the Municipal Water Authority of Aliquippa in November 2023. These attacks brought awareness to glaring gaps in the security of OT devices and demonstrated how geopolitical conflicts can have direct effects on the water and wastewater sector.

### **Related Groups**

Storm-0784 (Microsoft), Intrepid Jackal (CrowdStrike), UNC5691 (Mandiant), Bauxite (Dragos), ICTUS Team, BiskooitPedar, Tapesh Security Team, Cyber Av3ngers, Soldiers of Solomon.

### **Sectors of Interest**

Water, Government, Energy, Transportation, Oil & Gas, Technology.

### **Capabilities**

This group is typically considered low-skilled because of its more-unsophisticated tactics relying on discovering internet-exposed PLCs and utilizing default credentials to gain access. However, this last December saw the group employing **sophisticated** tactics, including the development of the IOControl malware used to infiltrate industrial control systems and internet-of-things (IOT) devices globally.

### **Sample of TTPs (MITRE ATT&CK)**

Default Accounts, Account Access Removal, Stored Data Manipulation, Loss of View, Internet Accessible Device, Loss of Availability. 💧

# BLENDING THREAT – Anti-Government Extremist Group Claims Credit for Weather Radar Sabotage, Calls for Further Action

Domestic violent extremists (DVEs) continue to call for attacks on U.S. critical infrastructure to further their malicious ideological agenda and disrupt the normal functioning of society. Over the summer, a sabotage attack against a weather radar station in Oklahoma underscored how hostile online rhetoric can lead to real world violence.

In July 2025, Oklahoma state authorities **charged** an individual for allegedly sabotaging a weather radar system. The **attack** temporarily knocked the radar offline. The individual is reportedly a member of **Veterans on Patrol** (VOP)—an anti-government violent extremist group—that believes government weather radars are a “weather weapon controlled by the military.” VOP incorporates anti-government beliefs and conspiracy theories related to **QAnon** and immigration into its ideological worldview. The group’s leadership wrote in repeated messages on Telegram that the equipment was “poisoning our skies.”

In May, the National Oceanic and Atmospheric Administration (NOAA) emailed its staff warning that the extremist group is recruiting people for “penetration drills” on locations hosting Next Generation Weather Radar (NEXRAD) systems. Prior to that, VOP shared images of radar sites, encouraging followers to investigate whether the equipment can be “easily sabotaged.” Moreover, the leader of VOP reportedly told **local media** that his group was responsible for the July Oklahoma attack. The group’s leader claimed VOP was watching Oklahoma radars closely. “We have these towers on observation, we’ve seen the security increases they are making to protect them,” he said. VOP’s leader claimed beefed-up security to protect the radars would not deter the group’s work. “Our goal is to take out 15 energy weapons in this state, and we want to do it simultaneously.”



The group is also reportedly responsible for doxxing multiple government officials in Washington state and claimed to have sabotaged a military vehicle assisting with Hurricane Helene relief efforts in North Carolina. This case is a classic example of a **blended threat** since physical attacks against these radar systems could hinder awareness and preparedness of natural hazard threats, thereby exacerbating the impact of extreme weather events. 💧

## Additional Reading:

- [A militarized conspiracy theorist group believes radars are ‘weather weapons’ and is trying to destroy them](#)
- [Weather Service staff urged not to visit sites alone after threats from militia group that believes radars are ‘weather weapons’](#)
- [Assessment of the Global Terrorism Threat Landscape in Mid-2025](#)

# OPERATIONAL RESILIENCE – Strengthen Your Supply Chain with EPA’s Supply Chain Resilience Resources

Supply chain disruptions can emanate from a variety of contingencies and lead to significant operational impacts for water and wastewater utilities. Utilities can help reduce the risk of supply chain shocks by understanding their supply chain dependencies and planning for disruptions.

The dynamic all-hazards threat landscape can induce supply shocks in several domains. During COVID-19, for example, supply chain disruptions **threatened the supply of chemicals** necessary to treat drinking water and wastewater. In 2022, the Russia-Ukraine war **impacted access to energy by increasing prices**, notably in Europe. A potential **Chinese invasion of Taiwan** would certainly disrupt trade between the U.S. and Asia. On the domestic front, water and wastewater utilities faced a threat to their supply chain from a **fire at a chemical manufacturing facility** in 2023, as well as threats to transportation networks **from striking workers**.



To help mitigate the risk of supply chain shocks, EPA’s Office of Water Emergency Response and Cybersecurity (OWERC), as the Sector Risk Management Agency for the water and wastewater sector, offers several free resources, products, and services, including case studies that offer best practices to help utilities enhance their supply chain resilience.

Utilities are encouraged to review EPA’s “**Supply Chain Resilience Guide for Water and Wastewater Utilities**,” which provides actions to prepare for, or respond to, both equipment and water treatment chemical supply chain challenges. Through best practices, utility case studies, and EPA resources, the Guide provides information that utilities can use to mitigate the impacts of a future supply chain disruption.

EPA also offers a series of additional products that can be used to help the water and wastewater sector enhance resilience to supply disruptions:

- **Water Treatment Chemical Supply Chain Profiles:** Provides a description of the supply chain for chemicals directly used in water treatment or used to manufacture water treatment chemicals.
- **Chemical Suppliers and Manufacturers Locator Tool:** Allows utilities to search for suppliers and manufacturers across the U.S. that may be able to fulfill their chemical supply need.
- **Current and Potential Supply Chain Disruptions website:** Provides up-to-date information on supply disruptions that could significantly impact the water and wastewater sector.
- **Safe Drinking Water Section 1441 website and Defense Production Act website:** Provides information on federal authorities that can be used to seek relief in the event of a critical supply shortage.

EPA can also provide one-on-one support to utilities through supply chain resilience technical assistance (TA). To request additional information about the assessment process, or to indicate interest in participating with an assessment, please email EPA at: [SupplyChainSupport@epa.gov](mailto:SupplyChainSupport@epa.gov).

WaterISAC and EPA encourage utilities to share any supply chain impacts they experience. In addition to the state primacy agency (and any other entity required by regulations), utilities can report a supply chain disruption to EPA at [SupplyChainSupport@epa.gov](mailto:SupplyChainSupport@epa.gov). WaterISAC also encourages utilities to report supply chain disruptions by emailing [analyst@waterisac.org](mailto:analyst@waterisac.org) or calling (866) H2O-ISAC.

*[Read more about supply chain resilience and access EPA’s free 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](mailto:Water-NSISB@epa.gov)

### WaterISAC

- Website | [www.waterisac.org/](http://www.waterisac.org/)
- Membership Information | [www.waterisac.org/membership](http://www.waterisac.org/membership)
- Incident Reporting Form | [www.waterisac.org/report-incident](http://www.waterisac.org/report-incident)
- 24 Hour Line | 866-H2O-ISAC

### EPA

- Office of National Security | [www.epa.gov/national-security](http://www.epa.gov/national-security)
- Drinking Water and Wastewater Resilience Website | [www.epa.gov/waterresilience](http://www.epa.gov/waterresilience)
- Cybersecurity for the Water Sector | <https://www.epa.gov/cyberwater>

### Water Sector Coordinating Council

- [American Water Works Association \(AWWA\)](#)
- [Association of Metropolitan Water Agencies \(AMWA\)](#)
- [National Association of Clean Water Agencies \(NACWA\)](#)
- [National Association of Water Companies \(NAWC\)](#)
- [National Rural Water Association \(NRWA\)](#)
- [Water Environment Federation \(WEF\)](#)
- [WaterISAC](#)
- [Water Research Foundation \(WRF\)](#)