



SAMANTHA F. RAVICH & TREVOR LOGAN

CHAIR & RESEARCH ANALYST, CENTER ON CYBER AND TECHNOLOGY INNOVATION,
FOUNDATION FOR DEFENSE OF DEMOCRACIES

IT'S TIME TO TALK ABOUT THE SHORTCOMINGS OF CYBERSECURITY IN THE WATER INDUSTRY

In the United States, there are 16 “critical infrastructure” sectors so vital for the fundamental health, safety, and prosperity of the country that their incapacitation or destruction would have catastrophic or even existential effects on the nation. The water sector may be the most crucial.

Over the last two decades, water utilities have incorporated automation technologies to provide reliable water to the public. However, this digitization has also exposed them to malicious cyber actors looking to deny or disrupt services.

The threat is not theoretical. From Atlanta to Seattle, America’s water systems are under sustained attack. In August 2021, malicious cyber actors deployed ransomware against a California-based wastewater facility. Earlier that year, hackers breached two Maine-based facilities. Probably the most well-known attack occurred one year ago when a hacker accessed and briefly manipulated the chemicals used to treat drinking water for the city of Oldsmar, Florida.

At the Foundation for Defense of Democracies’ Center on Cyber and Technology Innovation, we recently published a report warning of the significant cybersecurity deficiencies in drinking water and wastewater systems. We urged the U.S. government to devote more resources and collaborate more closely with industry to move the entire sector in the right direction.

Our fundamental belief is that governments must help empower the businesses, localities, and entities at the heart of the sector as opposed to creating more top-down government bureaucracy. With the large numbers of water utilities in the United States, this is the only path that can yield a timely and efficient outcome.

National governments around the world should establish grant programs for initiatives that bolster cybersecurity resilience. Cybersecurity grants are particularly beneficial for smaller and rural water organizations that may otherwise not have the budget or capacity to invest in cybersecurity. This may

seem like an obvious fix to a long-standing problem. However, of the U.S. federal government’s grants and low-interest loans to water utilities, Washington has spent less than one percent on cybersecurity projects.

Governments must also resource and organize their own agencies to be able to provide expertise and technical assistance to secure the water sector from physical and cyber threats. In the United States, this is the job of the Environmental Protection Agency, but for decades the agency has fallen short.

Better public-private collaboration between the water industry, threat information sharing institutions, and the intelligence community are necessary. Pairing operational knowledge of specific water facilities by private actors with government expertise on evolving trends in cyberattacks and defense can

facilitate timely and concrete action to protect vital water and wastewater systems.

Countries should consider establishing a joint industry-government oversight program to increase the cybersecurity of the water sector. The hallmark of this partnership is for industry experts to identify the technical standards for the water

organizations, while the respective governments can provide support and, if necessary, enforcement of regulations to ensure that a baseline of cybersecurity readiness and investment is met.

Since antiquity, poisoning of an enemy’s water source was a tried-and-true strategy to sow terror and decimate a population. The modern equivalent is now playing out in the targeting of the cyber backbone of the water sector. This essential lifeline sector itself will need to recognize its vulnerabilities and take long overdue measures to bolster its cyber defenses. The time for governments to make significant investments into cybersecurity for the water sector has arrived. While there will be other vital sources clamoring for scarce funding, expertise, and other resources, countries should keep in mind a sobering fact: A person can survive without water for only 3 days.

Governments must help empower businesses, localities, and entities at the heart of the sector as opposed to creating more bureaucracy