

Why hackers are targeting America's water systems and what ASU is doing about it

In this Q&A, cybersecurity expert Ozgur Ozmen explains the vulnerabilities behind recent attacks on critical infrastructure

By Kelly deVos, ASU News
August 11, 2026

Cyberattacks [targeting water](#) systems across the United States have exposed vulnerabilities in the technology controlling critical infrastructure.

While drinking water has remained safe, recent incidents have disrupted operations, caused water pressure losses and forced utility workers to intervene manually, [raising questions](#) about what could happen if a future attack goes further.

[Ozgur Ozmen](#), an assistant professor of computer science and engineering in the [School of Computing and Augmented Intelligence](#), part of the [Ira A. Fulton Schools of Engineering](#) at Arizona State University, studies the security of cyberphysical systems, where computers interact with physical devices and processes.

In this Q&A, Ozmen explains why water systems can be vulnerable to hackers, how cyberattacks can create real-world consequences and what ASU is doing to train the cybersecurity workforce needed to protect them.

Question: What makes water infrastructure an attractive — and potentially vulnerable — target for hackers?

Answer: There are two aspects: why these systems are attractive and why they are vulnerable.

Why they are attractive is straightforward. Water systems are critical to almost everything we do in our daily lives. We depend on water for drinking, agriculture and even data centers, which rely on water for cooling. Water is an extremely important resource for everyday life.

If you consider hackers who are trying to cause chaos or disrupt everyday life, water infrastructure is a very attractive target for achieving that.

Why are these systems vulnerable? Because they are very diverse and decentralized. Even small municipalities have their own water infrastructure. From my research, there are more than 170,000 water systems around the United States. It's very difficult to ensure that every one of these systems is secure from a cybersecurity perspective. With infrastructure operating at that scale, there are inevitably systems that remain vulnerable.

Q: Many of the systems targeted in these attacks control physical equipment such as pumps, valves and water pressure. How is an attack on this kind of cyberphysical system different from the cyberattacks people may be more familiar with?

A: The main difference is the physical impact.

When someone hacks your computer through malware or ransomware, the consequences generally remain in the digital domain. Your digital information might be stolen, or an attacker might encrypt your information and demand a ransom.

When you attack a cyberphysical system, there can be physical consequences. In these water infrastructure attacks, there were relatively small-scale physical impacts, such as service disruptions. But there could potentially be much more serious consequences, such as contaminating water.

Different cyberphysical systems create different potential consequences. With autonomous vehicles, an attacker could cause vehicle crashes. With smart grids, an attacker could disrupt electricity.

Attackers may use techniques similar to those used to compromise a traditional computer. The difference is that once they compromise the computers controlling a cyberphysical system, they can potentially affect the physical processes operated by those computers. There are parallels between traditional cybersecurity and cyberphysical security, but the biggest difference is the consequence.

Q: Reports suggest attackers have been able to exploit relatively basic weaknesses, including internet-connected equipment and weak or default passwords. Why do vulnerabilities like these persist in critical infrastructure? Is artificial intelligence, or AI, changing anything?

A: These types of vulnerabilities have been around for a long time. The [FBI](#) and the U.S. [Cybersecurity and Infrastructure Security Agency](#) have issued advisories against these practices. Programmable logic controllers, or PLCs, are small industrial computers. In a water system, they can control equipment such as pumps and valves, and help regulate processes like water pressure. These controllers shouldn't be exposed directly to the internet, and operators shouldn't use weak or default passwords.

But when you have tens of thousands of small-scale systems distributed around the United States, it's extremely difficult to ensure that every municipality follows cybersecurity best practices.

I would say the primary reasons we continue to see these vulnerabilities are the enormous scale of these systems and a shortage of cybersecurity experts who can advise smaller municipalities and help ensure they follow best practices.

AI adds another dimension. I think devices are becoming more vulnerable in the AI era because AI makes attacks much more accessible to potential attackers. Of course, AI can also enable better defenses. But an attacker only needs to find one vulnerability to enter a system, while a defender has to address all of the vulnerabilities.

Related story

[AI is a cybersecurity problem — and also a solution](#)

If AI helps someone identify a single vulnerability in a camera or a water treatment system, that can enable an attack. AI is lowering the barrier to becoming a bad actor in the cyber domain and potentially enabling attacks on a larger scale.

Q: Drinking water has remained safe in the recent incidents, but some communities have experienced disruptions such as pressure loss and have had to switch to manual operations. What does that tell us about the potential real-world consequences of a successful cyberattack on critical infrastructure?

A: These incidents showed that we still have some good fallback mechanisms. From what I have seen, manual intervention by operators prevented these attacks from becoming much larger issues.

But they also show that hackers were able to gain access to water infrastructure and cause some physical consequences. Those consequences could potentially have been much larger. An attack could contaminate water, for example, or it could go undetected.

We were fortunate to have personnel who were able to intervene at the correct moment and prevent these incidents from becoming larger. But whenever we depend on human intervention to prevent something, there is still the possibility of error. Those people might not have been available. They might not have been on site. There are many things that could have gone wrong and turned this into a much larger incident.

Ideally, that manual intervention shouldn't have been necessary in the first place. We still have a long way to go to address these vulnerabilities and make our infrastructure more resilient and secure.

Q: Cybersecurity is sometimes treated as something that can be added after a system has already been designed or deployed. Why is that approach particularly risky when we're talking about infrastructure that communities depend on every day?

A: One of the main things I tell my students is that you need to start with threat modeling. We need to identify what the threat is, what the attackers are trying to do, what capabilities they may possess and what assumptions we are making about our own system. Then we need to design our security mechanisms and our systems according to that threat model.

If we design a system using a weak threat model, underestimate the adversary or overestimate the security of our own system, the defenses we design can become vulnerable. That's where many vulnerabilities originate: We either overestimate our own security or underestimate the attacker's

capabilities.

If we do that work at the beginning, before designing our defenses and systems, we can prevent or mitigate many attacks. That's something I put a lot of emphasis on in my teaching and mentoring. We need to understand both the system and the adversary extremely well before we move on to designing defenses.

Q: Many local utilities have limited cybersecurity staff and resources, while the country more broadly faces a shortage of trained cybersecurity professionals. What happens when increasingly sophisticated threats collide with a workforce that may not have enough people to defend these systems?

A: One thing we need to understand is that cybersecurity is itself very interdisciplinary.

For instance, [I train students in cyberphysical system security](#). Hopefully, my students will be among the people who can help address attacks against water treatment plants, electrical infrastructure, autonomous vehicles or military drones. But there are very different aspects of cybersecurity. Other researchers work on operating-system security, for example, which is extremely important but very different from what I do.

We don't simply need more cybersecurity experts in general. We need experts in cyberphysical system security, network security, operating-system security, hardware security and many other areas. We need workforce development across all of those subdomains.

The scale of critical infrastructure makes the workforce challenge even more difficult. There are so many water treatment systems, including systems operated by very small municipalities, that it is difficult to ensure each one has a trained cybersecurity specialist.

That's also why [shorter courses and workshops](#) targeted toward working professionals can be important. We need ways to reach those professionals and give them the cybersecurity knowledge that can help prevent these issues in the future.

Q: Your research group gives students hands-on experience studying security vulnerabilities in cyberphysical systems, including IoT devices, sensors, robots and autonomous systems. How are you preparing students to protect the kinds of interconnected technologies that will increasingly make up our critical infrastructure?

A: That's something we're working on across the School of Computing and Augmented Intelligence. We are creating opportunities at every level so students can develop into the cybersecurity experts who will protect the next generation of technology. I [introduce middle school students to cybersecurity](#) through Desert CodeSprouts and mentor undergraduate researchers through the [Secure, Trusted, and Assured Microelectronics Center](#).

We also recently introduced a graduate course called [Intelligent and Safe Cyberphysical Systems](#). We address systems such as water treatment plants and smart grids in that course, so graduate students who take it can become more knowledgeable about these kinds of security issues.

We have to keep building that cybersecurity workforce pipeline because the technology and the threats will keep changing. Every new device and every new system create new security and privacy questions. If we give students opportunities to engage with those problems early and

continue developing their expertise, they can become the people we need to secure the critical systems our communities will depend on in the future.

This story originally appeared on [ASU News](#).

Main image



Instrumentation monitors pH and water flow in a water treatment system. In the School of Computing and Augmented Intelligence, part of the Ira A. Fulton Schools of Engineering at Arizona State University, researchers are exploring ways to better protect these systems and train students for high-impact infrastructure security roles. Photo by Erika Gronek/ASU