Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

Iran-affiliated and pro-Russia cyber actors gained access to and in some cases have manipulated critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors in late 2023 and 2024. These attacks highlight a potential public safety threat and an avenue for malicious cyber actors to cause physical damage and deny critical services. Outdated software, poor password security, the use of default credentials, and limited resources for system updates render ICS devices vulnerable to compromise, as they are commonly connected to corporate IT networks and increasingly to the Internet. Many operators face numerous competing priorities, such as physical facilities operations and maintenance, which further constrains the time and resources that operators can dedicate to cybersecurity practices. Furthermore, the limited number of ICS vendors, wide availability of product configurations, and operational commonalities across the water sector make it easier for cyber actors to compromise vulnerable systems.

IRGC-affiliated "Cyber Av3ngers" compromise Unitronics programmable logic controllers (PLCs)

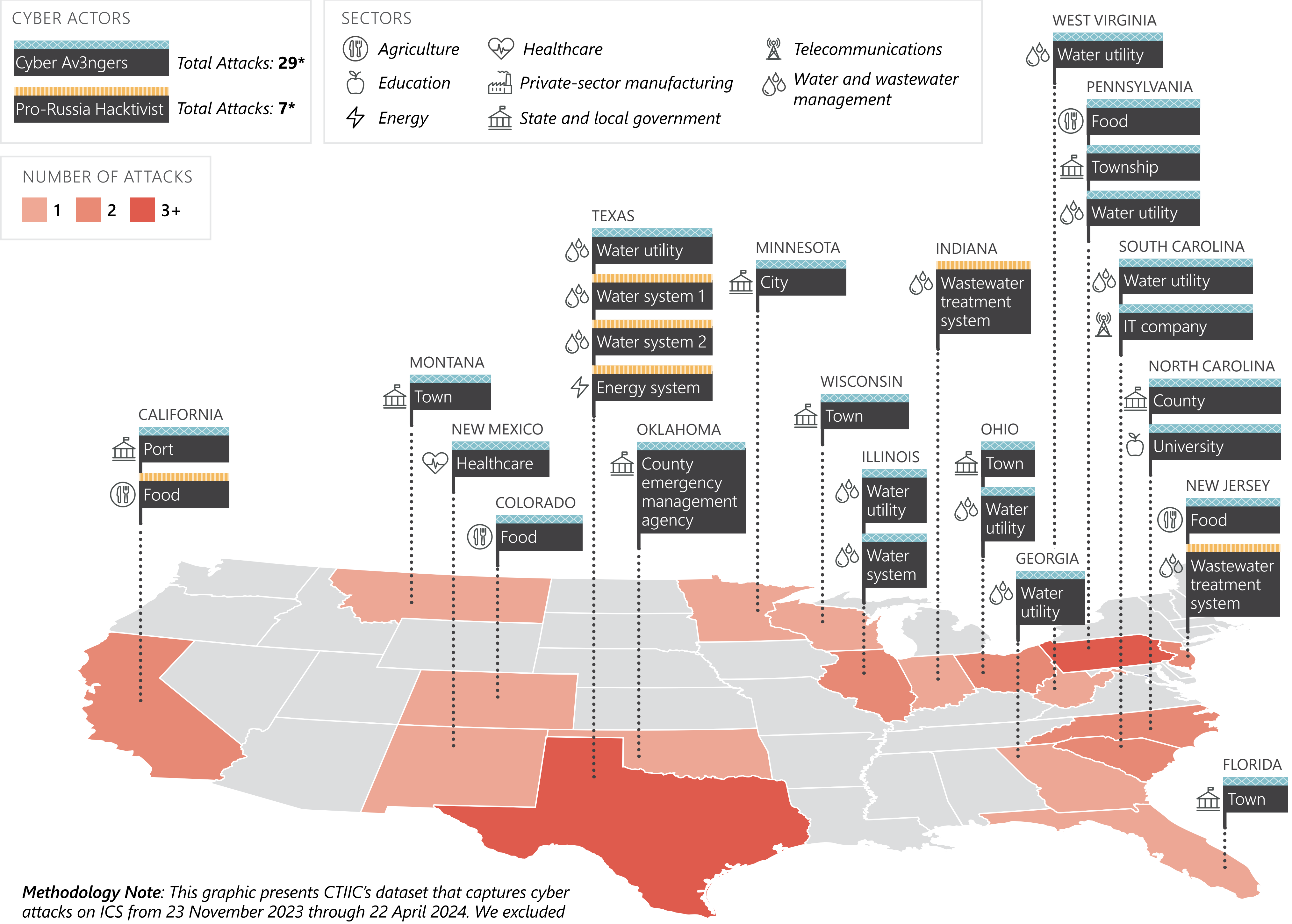
In November 2023, IRGC-affiliated actors operating under the Cyber Av3ngers persona gained access to the Israeli-made Unitronics Series ICS PLCs in multiple US entities, mostly water and wastewater systems, and defaced the PLCs' touch screens with an anti-Israel message. In response to the defacement, a few of the water-sector victims briefly shut down their systems and switched to manual operations.

Pro-Russia hacktivist compromised several water plants and claimed to compromise two dairies

A pro-Russia hacktivist remotely manipulated control systems within five water and wastewater systems and two dairies. The actors have typically accessed the ICS components via control interfaces with public-facing IP addresses.

- On 20 and 24 April 2024, the group posted videos showing an attacker remotely manipulating settings on human-machine interfaces (HMIs) within two US wastewater systems and one purported US energy company.
- On 18 January 2024, the group accessed control systems at two Texas water facilities and tampered with their water pumps and alarms, causing water to run past designated shutoff levels and overfill storage tanks.
- On 23 and 27 November 2023, the group also claimed on its public Telegram channel that it had attacked two US dairy systems.

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024

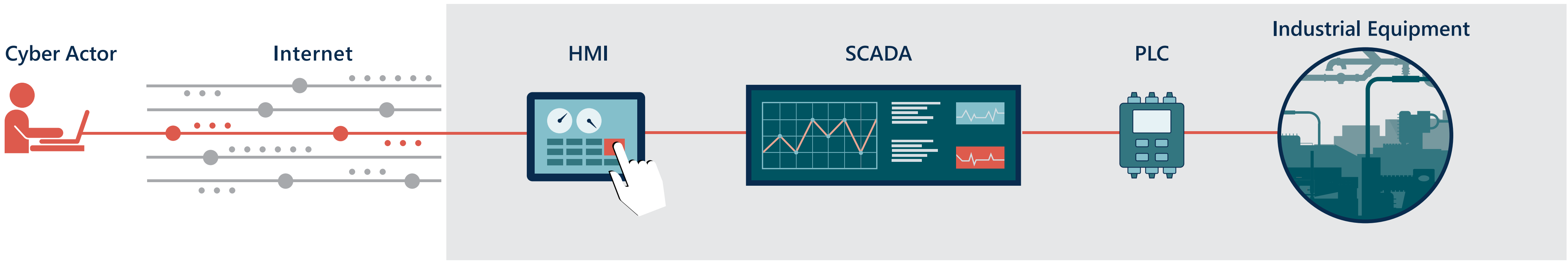


***Methodology Note**: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.*

*Including seven attacks at additional US locations.

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

CYBER ACTOR ATTACKS ICS INFRASTRUCTURE



CYBER DEFENSE BEST PRACTICES FOR UTILITIES

The following guidance is recommended by Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), FBI, Water Information Sharing and Analysis Center (WaterISAC). The top four recommendations will provide a critical reduction in the ICS attack surface.

TOP RECOMMENDATIONS

- Change Default Passwords Immediately
- Inventory ICS Assets To Find Vulnerable Devices and Manage Associated Common Vulnerabilities & Exposures (CVEs)
- Enforce User Access Controls and Multifactor Authentication for Remote Access
- Conduct a Cybersecurity Risk Assessment Focused on Reducing Exposure to the Public-Facing Internet

- Install Independent Cyber-Physical Safety Systems
- Conduct Regular Cybersecurity Assessments and Cybersecurity Awareness Training
- Develop and Exercise Cybersecurity Incident Response and Recovery Plans
- Develop and Enforce Cybersecurity Policies and Procedures (Governance)
- Implement Threat Detection and Monitoring
- Back Up ICS
- Integrate Cyber and Physical Incident Response, Mitigation, and Recovery Plans
- Participate in Information Sharing and Collaboration Communities

KEY TERMS

Industrial Control Systems (ICS)

ICS are a category of Operational Technology (OT) that focus on automating or remotely controlling physical processes. This is in contrast to Information Technology (IT), which focuses on manipulating, recording, and conveying data.

Some Types of ICS

SCADA
Supervisory control and data acquisition (SCADA) systems are large-scale distributed measurement and control systems designed to collect field information, transfer it to a control center, and display the information for monitoring. SCADA systems are used in the transmission and distribution of electricity, gas, oil, and water.

DCS
Distributed control systems (DCS) are computerized systems of controllers spread throughout a processing plant that allow for remote monitoring and supervision at various operational intervals to avoid having one potential point of failure. DCS are used in power generation, chemical processing, oil refining, and wastewater treatment.

Some Common ICS Hardware

HMI
A human machine interface (HMI) is a graphical control panel that displays different functions and data elements of ICS for human review and control.

PLC
A programmable logic controller (PLC) is a small industrial computer responsible for executing specific physical subprocesses, such as logic, timing, counting, communication, and data and file processing.