How the U.S. can defend its critical infrastructure

Washington Times, Page B1, By Amy McAuliffe, August 15, 2026

The recent cyberattacks, probably by Iran, against the technology that controls water and wastewater systems in at least 12 U.S. states is a stark reminder that America must do more to defend its critical infrastructure. They highlight the case for congressional action to reauthorize and expand key legislation, including one law that funds state and local efforts to harden this infrastructure.

We should not underestimate the threat from Tehran. Yet the most sophisticated cyber threat to more parts of the U.S. critical infrastructure comes from China.

China is lying in wait with pre-positioned cyber tools lurking in U.S. critical infrastructure, including water plants, power grids, communications systems and transportation hubs. Beijing's goal is to delay or deter U.S. intervention in a Pacific conflict.

The risk is that Beijing will use cyber tools to shut down American logistical, water, power or financial systems as it begins an invasion of Taiwan. China's strategic goal would be degrading U.S. resolve to intervene.

The days of experts debating whether China is engaging in these activities are over. Private-sector and U.S. government revelations about the Chinese-linked group Volt Typhoon demonstrated that China has already compromised these systems in the U.S. and Guam, a hub for American operations in the Pacific.

This is not a typical national security problem. Private companies, state and local governments and nonprofits own the majority of U.S. critical infrastructure, although ownership varies by sector.

Bipartisan cooperation and synchronized congressional and executive actions can help ensure that the federal government, state and local authorities and private-sector providers have tools to combat the threat from sophisticated, state-level cyber actors such as China.

Congress should expand grants and loans for state and local cybersecurity efforts; reauthorize key information sharing protections and enable the U.S. government to set minimum cybersecurity standards for crucial industries.

Without congressional action, an important cyber defense grant and loan program for state and local entities will expire in September. Experts at the state level view the program as a powerful tool in improving their baseline cyber defense capabilities.

States need continued access to these resources to keep up with the threat. Pending legislation (H.R. 5078) to reauthorize and expand the grant and loan program would help state and local entities guard against threats.

The bill expands grants to safeguard systems that control the switches, valves and circuits in critical infrastructure and fund investments in artificial intelligence-based cybersecurity systems.

Information sharing is also key, but provisions of the act that allow such sharing will expire next month absent congressional action.

Private companies now have the liability and antitrust protections they need to exchange information about cyber threats and incidents with each other and the government.

Congress should also empower the Cybersecurity and Information Security Agency to set minimum cybersecurity standards for critical sectors that rely on voluntary guidance. Water utilities are ripe for such standards. The largest and most critical operators should abide by the highest standards, while establishing streamlined, lower cost baselines for smaller municipal providers.

The executive branch also has a role to play. The U.S. strategy, spanning multiple administrations, of “naming and shaming” People’s Liberation Army and Chinese Ministry of State Security officials involved in cyberattacks has failed. Beijing generally responds by asking for more evidence or accusing the U.S. of a disinformation campaign. The Chinese government believes the U.S. will to respond is weak.

To change this dynamic, the U.S. should adopt a public declaratory cyber policy that would explicitly define U.S. critical infrastructure systems as off limits — and emphasize that any attack will trigger a disproportionate, cross domain response. We should pair the declaratory policy with a standing U.S.-China military and intelligence cyber dialogue to drive a deeper understanding of new U.S. red lines. Strengthening partnerships with allies that can detect Chinese intrusion campaigns from unique vantage points would be another powerful tool.

The Five Eyes alliance, an intelligence-sharing partnership on matters of national security among Australia, Canada, New Zealand, the United Kingdom and the U.S., has demonstrated its willingness to warn about cyber threats from China. The U.S. should also consider smaller allies. The Czech Republic, whose National Cyber and Information Security Agency has issued detailed public warnings about Chinese cyberattacks, is a strong candidate.

Amy McAuliffe is a distinguished visiting professor of the practice at the University of Notre Dame and a public speaker. She is a former CIA senior executive. The views she expresses are her own and not those of the U.S. government.