The Blue Front:
The Weaponisation of Water and America's Homeland Blind Spot

Dr Georgios Niveroglou

(Retired Brigadier General of the Hellenic Army and a former Director of the Military Office of the Minister of National Defence. He holds a doctorate from the National and Kapodistrian University of Athens, where he is now a postdoctoral researcher, and a master's degree in Applied Strategy and International Security from the University of Plymouth. His work focuses on the geopolitics of water, the security of critical infrastructure, and strategic communication.)

In the last days of July 2026, hackers reached into the operational technology of drinking-water utilities across at least a dozen American states[1] — among them Minnesota, Michigan, Georgia, South Dakota and New Jersey[2]. They changed administrator passwords, altered device settings and forced operators to fall back on manual control[3]. Boil-water notices followed in some jurisdictions; no contamination was confirmed. To most commentators this was a cybersecurity story about ageing controllers and weak passwords. It was, in fact, something larger. It was the moment the geopolitics of water stopped being a matter America observes abroad and became a front line running through the American homeland itself.

---

[1]Sam Sabin, 'The Number of States Targeted in Cyberattacks on Water Systems Has Jumped to 12', Axios, 4 August 2026, https://www.axios.com/2026/08/04/water-cyberattacks-us-iran.

[2]'What We Know So Far About the Hacking Campaign Against US Water Systems', Cybersecurity Dive, 20 August 2026, https://www.cybersecuritydive.com/news/what-we-know-so-far-about-the-hacking-campaign-against-us-water-systems/828374/.

[3]'Sweeping Cyberattack on Water Systems in Multiple States Has US Officials on Edge', CNN, 31 July 2026, https://www.cnn.com/2026/07/31/politics/sweeping-cyberattack-us-water-systems.

For a generation, Washington's strategic community has read "water conflict" as an affair of distant basins: the Nile, the Tigris–Euphrates, the Indus, the Mekong. That reading is no longer sufficient. Water has crossed a threshold — from a resource contested by the thirsty to an instrument wielded by the strong. It is now used deliberately, across both the physical and ***the cognitive domains***, by state actors who understand a simple truth: the surest way to reach an adversary's population is through the tap it trusts without a second thought.

From scarcity to statecraft

The familiar framing of water security is Malthusian. Populations grow, aquifers fall, rivers run thin, and scarcity drives communities and states towards conflict. That dynamic is real and it is worsening. But it captures only half of the present danger, and arguably the less urgent half. The sharper development of the past two years is not scarcity but control — the conversion of water, and of the infrastructure that moves and treats it, into a lever of coercion.

Three modalities of this coercion have now emerged with clarity. The first is hydraulic hegemony, the strategic exploitation of an upstream position. The second is the weaponisation of legal architecture, the suspension of the treaties that once made shared rivers predictable. The third, and the one that should most concern an American readership, is infrastructural sabotage — the direct manipulation of the systems that deliver water to homes, and with it the manipulation of public confidence. Examined together, they describe a domain of competition that the West has been slow to name.

Hydraulic hegemony: the view from the source

Whoever holds the source holds the option. Nowhere is this clearer than on the Tibetan Plateau, the water tower of Asia, from which the great rivers of the continent descend. On 19 July 2025, Premier Li Qiang presided over the groundbreaking of the Medog hydropower complex on the lower Yarlung Tsangpo, at the river's dramatic Great Bend. The project — five cascade dams with a projected capacity of roughly sixty gigawatts, some three times the output of the Three Gorges — is the most ambitious hydropower undertaking ever attempted[4]. Downstream, the same river becomes India's Siang and Brahmaputra and Bangladesh's

[4]'What's Driving China's Mega Medog Hydropower Project?', The Diplomat, 7 February 2026, https://thediplomat.com/2026/02/whats-driving-chinas-mega-medog-hydropower-project/.

Jamuna, sustaining around 130 million people and supplying a substantial share of India's fresh water and hydropower potential.

Beijing presents Medog as clean energy and climate adaptation. The strategic reality is that it hands China physical command over the timing of a river on which a principal American partner depends. No water-sharing treaty binds the upper and lower riparians; the arrangement in force is a limited flood-season data exchange dating to 2006[5]. Control over timing is control over leverage — the capacity to aggravate a dry season or a monsoon flood, or merely to let a downstream neighbour know that the capacity exists[6]. ***Infrastructure has become statecraft,*** and an upstream dam is now a standing strategic instrument rather than an engineering fact.

The weaponisation of legal architecture

If Medog shows how physical geography is turned into leverage, the Indus basin shows how legal architecture is dismantled to the same end. The Indus Waters Treaty of 1960, brokered by the World Bank, was for six decades the textbook example of durable water cooperation, surviving three wars between India and Pakistan[7]. That example no longer holds. On 23 April 2025, the day after the Pahalgam attack, India placed the treaty in abeyance, and New Delhi has since held that it will remain suspended until Pakistan verifiably ends its support for cross-border terrorism[8]. In August 2026 the Court of Arbitration at The Hague ruled that the treaty remained legally in force and that India's unilateral suspension carried no validity; New Delhi rejected the award outright — as it had the tribunal's earlier rulings — holding the court to be illegally constituted[9].

---

[5]'China's Mega Dam on Brahmaputra: Implications for India–China Relations', VisionIAS, 21 July 2025, https://visionias.in/blog/current-affairs/chinas-mega-dam-on-brahmaputra-implications-for-india-china-relations.

[6]'China's Medog County Mega-Dam Is Bad News for India and Bangladesh', Lowy Institute – The Interpreter, 6 February 2025, https://www.lowyinstitute.org/the-interpreter/china-s-medog-county-mega-dam-bad-news-india-bangladesh.

[7]Indus Waters Treaty 1960, signed at Karachi, 19 September 1960, 419 UNTS 125.

[8]'The Case for India's Suspension of the Indus Waters Treaty', The National Interest, 3 July 2026, https://nationalinterest.org/blog/silk-road-rivalries/the-case-for-indias-suspension-of-the-indus-waters-treaty.

[9]Permanent Court of Arbitration, The Indus Waters Western Rivers Arbitration (Islamic Republic of Pakistan v. Republic of India), PCA Case No. 2023-01, award of August 2026, https://pca-cpa.org/en/news/pca-press-release-pca-case-no-2023-01-the-indus-waters-western-rivers-arbitration-islamic-republic-of-pakistan-v-republic-of-india/; for contemporaneous reporting, 'India Rejects Court Order to Uphold Decades-Old Water-Sharing Treaty With Pakistan', CNBC, 1 September 2026, https://www.cnbc.com/2026/09/01/india-hague-ruling-pakistan-water-treaty.html.

The wider significance travels well beyond South Asia. When the most resilient water treaty in the world can be suspended as coercive leverage between two nuclear-armed states — and when Pakistan's own defence minister frames water as a matter of national survival for which his country would go to war[10] — the deterrent value of the entire legal scaffolding of transboundary water is called into question. That even a binding ruling of an international tribunal has not moved the parties only sharpens the point. Every downstream state now has reason to doubt that a treaty will protect it when relations sour. That is not a regional curiosity. It is a precedent, and precedents are contagious.

The homeland front: sabotage and its cognitive payload

The third modality is the one that has now arrived on American soil. The technique behind the 2026 intrusions was not sophisticated; it was exposure. Attackers reached programmable logic controllers left directly accessible on the public internet — in the observed cases, internet-exposed Rockwell devices — logged in against default or weak credentials, changed passwords to lock operators out, and altered settings[11]. The pattern echoed the 2023 compromise of a Pennsylvania municipal water authority attributed to CyberAv3ngers, a group affiliated with Iran's Islamic Revolutionary Guard Corps; officials stopped short of formally attributing the 2026 wave, but analysts again pointed to an Iranian nexus[12].

Beneath this opportunistic activity lies a graver and more patient threat. Since at least early 2024, United States agencies have assessed with high confidence that the Chinese state-sponsored group known as Volt Typhoon pre-positioned itself inside American critical-infrastructure networks, water among them — not to spy, but to be able to disrupt those

[10]'Indus Water Treaty Becomes Latest India–Pakistan Flashpoint', CNBC, 22 June 2026, https://www.cnbc.com/2026/06/22/india-pakistan-indus-waters-treaty-water-dispute-war-risk.html.

[11]Cybersecurity and Infrastructure Security Agency, 'Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure', Joint Cybersecurity Advisory AA26-097A, 7 April 2026 (updated July 2026), https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a; on the 2023 antecedent, Cybersecurity and Infrastructure Security Agency, 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities', Joint Cybersecurity Advisory AA23-335A, 1 December 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

[12]'What to Know About the U.S. Water Systems Cyberattacks', Time, 2 August 2026, https://time.com/article/2026/08/02/what-to-know-about-the-u-s-water-systems-cyberattacks/.

systems during a future crisis[13]. The purpose is widely read as coercive: to slow or deter American intervention in a Pacific contingency over Taiwan by threatening the lifelines of the home front[14]. Two threat models therefore run in parallel — Iranian coercion for signalling and retaliation, Chinese pre-positioning for strategic denial — and both converge on the same soft target.

Here the analysis must go one step further than most cybersecurity commentary allows, because the physical damage so far has been modest — lost pressure, precautionary notices, no poisoning of a single glass of water. If disruption were the sole objective, the campaign under-performed. But disruption is not the sole objective. Water is the one piece of infrastructure that every citizen consumes bodily, daily, and on trust. An adversary who can make Americans wonder whether the water from their own tap is safe achieves a psychological effect out of all proportion to the technical harm inflicted. ***The message is unambiguous: we can reach you where you are most intimate and least defended.***

This is the convergence Western planning has been slow to grasp. In the water domain the kinetic and the cognitive are fused: a minor technical incident is a major narrative event, and the true target is not the reservoir but public confidence in it. Deterrence calculations that price only physical damage therefore misread the currency being contested. ***The attack on the controller is the vector; the attack on trust is the payload.***

The American blind spot

For a generation, Western strategic planning has treated water conflict as largely exogenous — a hardship of arid regions and fragile states, to be managed through aid and diplomacy. America's adversaries have quietly inverted that assumption. The reasons water is so exposed are structural and, once stated, obvious. It is indispensable and irreplaceable, so any credible threat to it commands attention. It is radically decentralised: the country is served by tens of thousands of mostly small, locally run community systems, for which cybersecurity competes

[13]Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation, 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure', Joint Cybersecurity Advisory AA24-038A, 7 February 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[14]Amy McAuliffe, 'How the U.S. Can Defend Its Critical Infrastructure', The Washington Times, 13 August 2026, https://www.washingtontimes.com/news/2026/aug/13/us-defend-critical-infrastructure/.

for scarce funds against schools and roads[15]. It is rich in unglamorous, poorly defended targets. And, as argued above, it yields a cognitive return far exceeding the physical effort required. No other critical sector combines these properties so completely.

Towards deterrence and resilience

Treating this as a run of unfortunate IT incidents would compound the error. Five lines of effort follow from reading water as strategic terrain rather than a utilities problem.

First, reclassify. Water should be integrated explicitly into the national deterrence posture, not left to environmental and public-health authorities alone. A sector that adversaries treat as a battlespace cannot be defended as a service.

Second, mandate and fund. Enforceable baseline standards for operational-technology security — segregating controllers from the public internet, eliminating default credentials, rehearsing manual fallback — are overdue[16]. But a baseline imposed on a town of eight thousand people without the money to meet it will not hold; the mandate and the means must travel together.

Third, share intelligence downward. Threat information must reach the small operators who at present too often learn of a campaign from the evening news. A sector-specific channel that pushes warning to the least-resourced utilities, rather than merely collecting reports from them, is the practical test of seriousness.

Fourth, raise the cost. Adversaries pre-position precisely because doing so is cheap and consequence-free. Resilience — redundancy, rapid recovery, credible manual operation — raises the cost of disruption; a clear declaratory policy that names intrusions into water systems for what they are, and attaches consequences to them, raises it further. Deterrence by denial and deterrence by cost are complementary, not alternatives.

Fifth, and most neglected, ***defend the cognitive line***. If the payload is public trust, then resilience must include the pre-emptive communication that lets the narrative fail even when an intrusion succeeds. Utilities and authorities that can tell the public quickly and credibly

---

[15] Sabin, Axios, op. cit.

[16] 'What We Know So Far…', Cybersecurity Dive, op. cit.

that the water is safe deny the adversary the very effect it seeks. In this domain, communication is not public relations; it is force protection for the population.

There is, finally, ***a transatlantic dimension that Athens and Washington should not overlook***. European water systems rest on the same architecture and face the same adversaries; the Alliance's resilience agenda, grounded in the Article 3 commitment and its Baseline Requirements, should name water as a critical sector in its own right and ***exercise water-disruption scenarios*** as it exercises energy and communications. One caution deserves emphasis above the rest: adversaries will strike the seam between the physical and the cognitive precisely because that is where allied planning remains thinnest.

Conclusion

Water has always been life. It is now also leverage, and increasingly a message. The states that grasp this first — that come to defend the tap as seriously as they defend the border — will hold an advantage in a competition whose front line now runs through the basement of every waterworks. America's adversaries have already begun to redraw the map. The advantage will lie with those — in Washington and among its allies — who read the new one first.

Bibliography

Primary sources

Cybersecurity and Infrastructure Security Agency, 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities', Joint Cybersecurity Advisory AA23-335A, 1 December 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation, 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure', Joint Cybersecurity Advisory AA24-038A, 7 February 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Cybersecurity and Infrastructure Security Agency, 'Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure', Joint Cybersecurity Advisory AA26-097A, 7 April 2026 (updated July 2026), https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a.

Indus Waters Treaty 1960, signed at Karachi, 19 September 1960, 419 UNTS 125.

Permanent Court of Arbitration, The Indus Waters Western Rivers Arbitration (Islamic Republic of Pakistan v. Republic of India), PCA Case No. 2023-01, https://pca-

cpa.org/en/news/pca-press-release-pca-case-no-2023-01-the-indus-waters-western-rivers-arbitration-islamic-republic-of-pakistan-v-republic-of-india/.

Publications and analyses

‘The Case for India’s Suspension of the Indus Waters Treaty’, The National Interest, 3 July 2026, https://nationalinterest.org/blog/silk-road-rivalries/the-case-for-indias-suspension-of-the-indus-waters-treaty.

‘China’s Medog County Mega-Dam Is Bad News for India and Bangladesh’, Lowy Institute – The Interpreter, 6 February 2025, https://www.lowyinstitute.org/the-interpreter/china-s-medog-county-mega-dam-bad-news-india-bangladesh.

‘China’s Mega Dam on Brahmaputra: Implications for India–China Relations’, VisionIAS, 21 July 2025, https://visionias.in/blog/current-affairs/chinas-mega-dam-on-brahmaputra-implications-for-india-china-relations.

‘India Rejects Court Order to Uphold Decades-Old Water-Sharing Treaty With Pakistan’, CNBC, 1 September 2026, https://www.cnbc.com/2026/09/01/india-hague-ruling-pakistan-water-treaty.html.

‘Indus Water Treaty Becomes Latest India–Pakistan Flashpoint’, CNBC, 22 June 2026, https://www.cnbc.com/2026/06/22/india-pakistan-indus-waters-treaty-water-dispute-war-risk.html.

McAuliffe, Amy, ‘How the U.S. Can Defend Its Critical Infrastructure’, The Washington Times, 13 August 2026, https://www.washingtontimes.com/news/2026/aug/13/us-defend-critical-infrastructure/.

Sabin, Sam, ‘The Number of States Targeted in Cyberattacks on Water Systems Has Jumped to 12’, Axios, 4 August 2026, https://www.axios.com/2026/08/04/water-cyberattacks-us-iran.

‘Sweeping Cyberattack on Water Systems in Multiple States Has US Officials on Edge’, CNN, 31 July 2026, https://www.cnn.com/2026/07/31/politics/sweeping-cyberattack-us-water-systems.

‘What to Know About the U.S. Water Systems Cyberattacks’, Time, 2 August 2026, https://time.com/article/2026/08/02/what-to-know-about-the-u-s-water-systems-cyberattacks/.

‘What We Know So Far About the Hacking Campaign Against US Water Systems’, Cybersecurity Dive, 20 August 2026, https://www.cybersecuritydive.com/news/what-we-know-so-far-about-the-hacking-campaign-against-us-water-systems/828374/.

‘What’s Driving China’s Mega Medog Hydropower Project?’, The Diplomat, 7 February 2026, https://thediplomat.com/2026/02/whats-driving-chinas-mega-medog-hydropower-project/.