How vulnerable is critical infrastructure to cyberattack in the US?

Our water, health, and energy systems are increasingly vulnerable to cyberattack.

Now, when tensions escalate — like when the US bombed nuclear facilities in Iran this month — the safety of these systems becomes of paramount concern. If conflict erupts, we can expect it to be a "hybrid" battle, Joshua Corman, executive in residence for public safety & resilience at the Institute for Security and Technology (IST), tells *The Verge*.

"With great connectivity comes great responsibility."

Battlefields now extend into the digital world, which in turn makes critical infrastructure in the real world a target. I first reached out to IST for their expertise on this issue back in 2021, when a ransomware attack forced the Colonial Pipeline — a major artery transporting nearly half of the east coast's fuel supply — offline for nearly a week. Since then, *The Verge* has also covered an uptick in cyberattacks against community water systems in the US, and America's attempts to thwart assaults supported by other governments.

It's not time to panic, Corman reassures me. But it is important to reevaluate how we safeguard hospitals, water supplies, and other lifelines from cyberattack. There happen to be analog solutions that rely more on physical engineering than putting up cyber firewalls.

This interview has been edited for length and clarity.

As someone who works on cybersecurity for water and wastewater, healthcare, food supply chains, and power systems – what keeps you up at night?

Oh, boy. When you look across what we designate as lifeline critical functions, the basic human needs – water, shelter, safety – those are among some of our most exposed and underprepared. With great connectivity comes great responsibility. And while we're struggling to protect credit card cards or websites or data, we continue to add software and connectivity to lifeline infrastructure like water and power and hospitals.

We were always prey. We were just kind of surviving at the appetite of our predators, and they're getting more aggressive.

How vulnerable are these systems in the US?

You might have seen the uptick in ransomware starting in 2016. Hospitals very quickly became the number one preferred target of ransomware because they're what I call "target rich, but cyber poor." The unavailability of their service is pretty dire, so the unavailability can be monetized very easily.

You have this kind of asymmetry and unmitigated feeding-frenzy, where it's attractive and easy to attack these lifeline functions. But it's incredibly difficult to get staff, resources, training, budget, to defend these lifeline functions.

If you're a small, rural water facility, you don't have any cybersecurity budget. We often usher platitudes of 'just do best practices, just do the NIST framework.' But they can't even stop using end of life, unsupported technology with hard-coded passwords.

"You have this kind of asymmetry and unmitigated feeding-frenzy"

It’s about 85 percent of the owners and operators of these lifeline critical infrastructure entities that are target rich and cyber poor.

Take water systems, for example. Volt Typhoon has been found successfully compromising US water facilities and other lifeline service functions, and it’s sitting there in wait, prepositioning. [*Editor’s note: Volt Typhoon is a People’s Republic of China state-sponsored cyber group*]

China specifically has intentions toward Taiwan as early as 2027. They basically would like the US to stay out of their intentions toward Taiwan. And if we don’t, they’re willing to disrupt and destroy parts of these very exposed, very prone facilities. The overwhelming majority don’t have a single cybersecurity person, haven’t heard of Volt Typhoon, let alone know if and how they should defend themselves. Nor do they have the budget to do so.

Turning to recent news and the escalation with Iran, is there anything that is more vulnerable at this moment? Are there any unique risks that Iran poses to the US?

Whether it’s Russia or Iran or China, all of them have shown they are willing and able to reach out to water facilities, power grids, hospitals, etc. I am most concerned about water. No water means no hospital in about four hours. Any loss of pressure to the hospital’s pressure zone means no fire suppression, no surgical scrubbing, no sanitation, no hydration.

What we have is increasing exposure that we volunteered into with smart, connected infrastructure. We want the benefit, but we haven’t paid the price tag yet. And that was okay when this was mostly criminal activity. But now that these points of access can be used in weapons of war, you could see pretty severe disruption in civilian infrastructure.

Now, just because you can hit it doesn’t mean you will hit it,

right? I'm not encouraging panic at the moment over Iran. I think they're quite busy, and if they're going to use those cyber capabilities, it's a safer assumption they would first use them on Israel.

Different predators have different appetites, and prey, and motives.

Sometimes it's called access brokering, where they're looking for a compromise and they lay in wait for years. Like in critical infrastructure, people don't upgrade their equipment, they use very old things. If you believe that you'll have that access for a long time, you can sit on it and wait patiently until the time and the place of your choosing.

Think of this a little bit like *Star Wars*. The thermal exhaust port on the Death Star is the weak part. If you hit it, you do a lot of damage. We have a lot of thermal exhaust ports all over water and healthcare specifically.

What needs to be done now to mitigate these vulnerabilities?

We're encouraging something called cyber-informed engineering.

What we've found is if a water facility is compromised, abrupt changes in water pressure can lead to a very forceful and damaging surge of water pressure that could burst pipes. If you were to burst the water main for a hospital, there would be no water pressure to the hospital. So if you wanted to say, 'let's make sure the Chinese military can't compromise the water facility,' you'd have to do quite a bit of cybersecurity or disconnect it.

What we're encouraging instead, is something much more familiar, practical. Just like in your house, you have a circuit breaker, so if there's too much voltage you flip a switch instead of burning the house down. We have the equivalent of circuit breakers for water, which are maybe $2,000, maybe under $10,000. They can detect a surge in

pressure and shut off the pumps to prevent physical damage. We're looking for analog, physical engineering mitigation.

"Think of this a little bit like *Star Wars*."

If you want to reduce the likelihood of compromise, you add cybersecurity. But if you want to reduce the *consequences* of compromise, you add engineering.

If the worst consequences would be a physically damaging attack, we want to take practical steps that are affordable and familiar. Water plants don't know cyber, but they do know engineering. And if we can meet them on their turf and help explain to them the consequences and then co-create affordable, realistic, temporary mitigations, we can survive long enough to invest properly in cybersecurity later.

Federal agencies under the Trump administration have faced budget and staffing cuts, does that lead to greater vulnerabilities as well? How does that affect the security of our critical infrastructure?

Independent of people's individual politics, there was an executive order from the White House in March that shifts more of the balance of power and responsibility to states to protect themselves, for cybersecurity resilience. And it's very unfortunate timing given the context we're in and that it would take time to do this safely and effectively.

I think, without malice, there has been a confluence of other contributing factors making the situation worse. Some of the budget cuts in CISA, which is the national coordinator across these sectors, is not great. The Multi-State Information Sharing and Analysis Center is a key resource for helping the states serve themselves, and that too lost its funding. And as of yet, the Senate has not confirmed a CISA director.

We should be increasing our public private partnerships, our federal and state level partnerships and there seems to be

bipartisan agreement on that. And yet, across the board, the EPA, Health and Human Services, Department of Energy and CISA have suffered significant reduction in budget and staff and leadership. There’s still time to correct that, but we are burning daylight on what I see as a very small amount of time to form the plan, to communicate the plan, and execute the plan.

Whether we want this or not, more responsibility for cyber resilience and defense and critical functions is falling to the states, to the counties, to the towns, to individuals. Now is the time to get educated and there is a constellation of nonprofit and civil society efforts — one of them is the good work we’re doing with this Undisruptable27.org, but we also participate in a larger group called Cyber Civil Defense. And we recently launched a group called the Cyber Resilience Corps, which is a platform for anyone who wants to volunteer to help with cybersecurity for small, medium, rural, or lifeline services. It’s also a place for people to find and request these volunteers. We’re trying to reduce the friction of asking for help and finding help.

I think this is one of those moments in history where we want and need more from governments, but cavalry isn’t coming. It’s going to fall to us.

https://www.theverge.com/cyber-security/693588/cybersecurity-cyberattack-critical-infrastructure-war-expert-iran