The Invisible Siege: State Sponsored Cyber Espionage and the Vulnerability of U.S. Infrastructure

Jacob Mullins

Applied Critical Thinking and Analysis

Professor Elena Mastors

Johns Hopkins University

May 10, 2024

Introduction:

Ransomware attacks are on the rise. There is a shift in focus toward critical infrastructure. Vital areas like utilities, communication, transportation, emergency response, healthcare, and government are attractive targets for hackers looking for higher probability of cashing in ransom payments. Reports of water treatment facilities being targeted have been circulating since November 2023, asserting an imminent Chinese cyber-attack. Who is really behind these cyber-attacks? What are they targeting, and what does that say about their intentions? How is the U.S. combatting these threats?

Threat Analysis:

News reports of cyber-attacks are growing in frequency and are expected to accelerate prior to the U.S. presidential election (Quillen 2024). Although headlines specifically warn of Chinese threats to water facilities, we are still uncovering the true breadth of Chinese cyber breaches, of which water is only a minor target. Their tactics, techniques, and procedures (TTP) are well choreographed, highly elusive, and focused on unusual targets (Cyber Security Advisory 2024).

Who is attacking U.S. Infrastructure?

- **Volt Typhoon** [state-sponsored by China]: Establishing *pre-positioning* for a potential future attack with broad access to diverse critical infrastructure.
    - Motive: Deter U.S. interference in Chinese conflicts.
- **Cyber Av3ngers** [Iran-based 'hacktivists']: Minor cyber-attacks executed against water treatment facilities (Walter 2023)
    - Motive: Anti-Israel sentiments.

- Anonymous independent actors: Successful ransomware attacks on critical infrastructures
    - Motive: Money

Anonymous actors are financially motivated, and Cyber Av3ngers are hacktivists who tend to exaggerate their achievements and effectiveness. Examining the results of their cyber-attacks will help us gauge the gravity of the threat posed by Volt Typhoon's positioning in U.S. infrastructure.

China claims Volt Typhoon is an unsponsored, decentralized, international hacking group (Fomenko 2024); however, Volt Typhoon appears not to be financially motivated like anonymous actors are, living inside systems for as long as five years without executing a ransom attack. Microsoft's intelligence analysts publicly attribute Volt Typhoon as a nation-state espionage group based out of China (Microsoft Threat Intelligence 2023).

Russia Today advocates for China's innocence claiming the timing of U.S. news reporting on Volt Typhoon is meant to sow distrust and undermine the diplomacy efforts of Xi Jinping on his visit to European countries in May 2024. This defense comes from a Russian state-sponsored, right leaning, low factuality rated news organization (Ground News 2024). After parroting China's denials of sponsorship, Fomenko tips his hand by committing a tu quoque fallacy, "Are we really going to pretend the CIA doesn't hack anyone?", giving China, and everyone else, a pass to commit cyber espionage on the U.S. since *they do it too* (Fomenko 2024). After Edward Snowden's revelations, China's perceptions that America used its privileged position in the cyber domain to 'perpetuate American hegemony' was probably reinforced (Inkster 2015), justifying any efforts made to launch a widespread cyber espionage campaign on the U.S.

Why is Volt Typhoon an intelligence threat?

“It is highly likely that in the next war, the first shot will be fired in cyber,” Brandon Wales, CISA Executive Director (Jonathan Greig 2024) CISA Assistant Director, Eric Goldstein, reports they have found hackers pre-positioning themselves in critical infrastructure where there is no reasonable espionage benefit. The most probable motive is to slow any potential mobilization of U.S. forces, and cause turmoil in the population.

For example, in January, emergency communications outside of Philadelphia were taken out by an anonymous ransomware actor, requiring dispatchers to use pen and paper. “If a foreign terrorist group, or a nation state, can tie up law enforcement responses by targeting their 911 Call center, or police departments can’t gain access to investigative or other important information – that will hamper their emergency response, and aid a threat actor in achieving their operational objectives.” (Josh Margolin 2024)

Cyber Av3ngers struck an Aliquippa, Pennsylvania water facility because their *Vision Series logic controller by Unitronics* is Israeli made, who Iran wanted to protest (Associated Press 2023). The dangers of cyber-attacks on water systems are potentially turning off water pumps or contaminating the water supply. Due to the manual redundancies and testing safeguards in place at these facilities, we have yet to experience a cyber-attack effective at causing public harm or panic (Associated Press 2024). Since Volt Typhoon is lying in wait, focused on collecting data and learning the systems they infiltrate, we expect they would be more effective at causing significant damage to their target.

“Federal departments and agencies assess with high confidence that Chinese sponsored group, Volt Typhoon, actors are pre-positioning themselves to disrupt critical infrastructure operations in the event of geopolitical tensions and/or military conflicts.” (Natter 2024) Drinking

water and wastewater systems are attractive targets because they are a lifeline sector that is under protected.

Which infrastructure is being targeted?

"The affected organizations span the **communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors."** (Microsoft Threat Intelligence 2023)

Volt Typhoon has not executed any attacks. (Cyber Security Advisory 2024) There is abundant evidence that Volt Typhoon has penetrated a wide variety of U.S. Infrastructure using highly concealed TTP, allowing them to dedicate resources to maintaining data extraction to study and understand the target environment over time.

What does China achieve with Volt Typhoon?

Since targets serve no espionage benefit, we conclude their intentions are to wait in case of a major conflict with the U.S. "It is not a 'this month' problem. It is going to be a problem for multiple years, and we are seeing Volt Typhoon activity every single day." -Morgan Adamski, director of NSA. (Waldman 2024) Volt Typhoon has maintained access to critical infrastructure IT environments for at least five years. They evade regular detection, so information sharing is critical in tracking their activity. Volt Typhoon uses Living of the Land (LOTL) techniques which means there isn't simply a list of breach indicators that can be distributed to detect their activity.

Why is the Environmental Protection Agency (EPA) being so vocal about Volt Typhoon?

The Aliquippa water system breach occurred weeks after the EPA lost a battle for cyber security funding, and since then have used it as political capital to gain funding support (Lyngaas

2024): “State Governments must improve their defenses against cyber threats.”, EPA Administrator Michael Regan and National Security Advisor Jake Sullivan said in their memo from the White House (Michael Regan 2024). The EPA is setting up a task force to identify the most significant vulnerabilities. Although it was Iranian hackers who breached the water facilities, the U.S. believes China will pull the trigger on their prepared cyber-attacks if we enter conflict with them.

How can we defend against Volt Typhoon?

Since Microsoft discovered the existence of these breaches, the government joined with the public sector to share information on detections and prevention of Volt Typhoon positions. There are now published trainings on the methodology required to discover these LOTL techniques including the development and practice of incident response plans, conducting regular Cybersecurity assessments, and reducing edge point exposure to the public internet. (Cybersecurity & Infrastrucure Security Agency 2024)

Maj. Gen Lorna Mahlock is confident this solidifies our upper hand when he says, “the U.S. has an asymmetric advantage and superpower in our industry partners, and we are not in the fetal position in a corner.” (Jonathan Greig 2024)

Conclusion:

Is China preparing for war? Probably, but with whom? It seems unlikely that China is intending to follow through on an attack on U.S. infrastructure given the severe response they should expect from the U.S. and our allies. However, it is credible that they will try using their cyber positioning as a knife to our throat in the event they pursue a major conflict elsewhere (like a Taiwan invasion) that the U.S. opposes.

What should we do? The intelligence community and the five eyes are combining efforts to create and distribute detailed guides to help critical infrastructures succeed in detecting Volt Typhoon activity such as the CSA Living off the Land report (Joint Cybersecurity Advisory 2023). The U.S. intelligence agencies need to continue cultivating the information sharing relationship they have with the public sector and other vulnerable infrastructure targets to improve our ability to discover of the scale of Volt Typhoon's penetration. The U.S. government has vastly superior cyber capabilities and combined with the support of Silicon Valley tech giants like Microsoft, we will prevail in any battle for control of our infrastructure in any cyber-attack.

Premortem Analysis:

What are the ways the above conclusions could be wrong?

- Were there alternative hypotheses not considered?
    - Could the U.S. be behind Volt Typhoon? If China does something like invade Taiwan, the U.S. could justify inaction claiming its hands are tied from providing military support due to the metaphorical gun *China* [U.S. framing them] would have pointed at us. America could give a legitimate reason to avoid a military conflict/loss of American lives that we didn't want to get involved in.
- Did external influences affect the outcome?
    - Are China's allies going to coordinate similar efforts to maximize the damage caused by a nationwide cyber-attack? Will Russia, North Korea, or Iran join in on an attack?
- Did deception go undetected?

    - Most likely. Volt Typhoon's major calling card is the depth of their deception, so it is likely that we are operating with an underestimate of their current cyber access and control. If they had the ability to permanently cripple U.S. infrastructure without warning, their threats would have more power when strong arming U.S. policymakers.
- Unreliable sources:
    - China and Russia are unreliable sources. There is little to be gained by listening to the messages they send verbally, since they have every incentive to push narratives that support their position and undermine their enemies.
    - It's likely that many at-risk targets will not heed the Intelligence Community's warnings or follow instructions diligently to successfully detect breaches. They may report to be clear of external attacks when they really were lazy in their searches.
- Was any contradictory evidence ignored?
    - Contradictory *claims* were ignored. Are Russia and China telling the truth? Is Volt Typhoon just an independent group working towards some unknown goal? If true, the U.S. could potentially overestimate the threats being posed, assuming they are some well-coordinated, centralized attack, when they are just an illegal data mining operation. Conversely, we could underestimate Volt Typhoon's risk tolerance, allowing them to take drastic actions all while leaving China to be blamed.
- Did the absence of information mislead us?

    - Is China just innocently gathering benign data for niche purposes? Not having overt admission leaves some uncertainty about the motives of Volt Typhoon.
- Were our key assumptions valid?
    - Is China's goal really to strong arm/ threaten the U.S.?
    - Is Volt Typhoon really an independent party? If so, what's deterring them from attacking at any time? Are they just selling the data they gather to U.S. adversaries, but have no intention to launch an attack?
    - Is Volt Typhoon capable of launching an effective cyber-attack against U.S. infrastructure? Or are they only able to gather data?
    - Does China plan on invading Taiwan?

This Premortem exercise highlighted several key areas where we lack certainty, and others where there are possible fail points. After this analysis, I would recommend the government enact specific incentives to any cyber security managers that find Volt Typhoon activity. This seemed like the most probable point of failure in the detection process: indifferent cybersecurity employees at small scale infrastructure facilities who let breaches go undetected.

Bibliography

Associated Press. 2024. "Cyber attack at municipal water authority in Pennsylvania prompts renewed cybersecurity warnings." *ABC News Station*, January 2. https://www.wnep.com/article/news/state/water-authority-hacked-pennsylvania-cybersecurity-warnings-federal-security-officials/523-1b311bd6-5f7c-416e-ac80-975e1a1447e1.

—. 2023. "Pa. water authority one of several organization breached by Iran-affiliated hackers, federal agencies say." *WHYY*, December 2. https://whyy.org/articles/pennsylvania-water-authority-breach-iran-affiliated-hackers/.

Cyber Security Advisory. 2024. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." *Cybersecurity & Infrastructure Security Agency*, February 7. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Cybersecurity & Infrastrucure Security Agency. 2024. "Top Cyber Actions for Securing Water Systems." *America's Cyber Defence Agency*, February 23. https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems.

Fomenko, Timur. 2024. "New hacking allegations against China aren't what they seem." *Russia Today*, April 4. https://www.rt.com/news/595310-china-hacking-us-uk/?utm_source=ground.news&utm_medium=referral.

Inkster, Nigel. 2015. "Cyber Espionage." *Adelphi series* 72. https://doi.org/10.1080/19445571.2015.1181443.

Joint Cybersecurity Advisory. 2023. *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.* Intelligence Threat, Washington, DC: National Security Agency. https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF.

Jonathan Greig, Martin Matishak. 2024. "Any number given of Volt Typhoon victims 'likely an underestimate,' CISA says." *The Record Media*, May 7. https://therecord.media/volt-typhoon-targets-underestimated-cisa-says.

Josh Margolin, Sasha Pezenik. 2024. "Emergency services a liely target for cyberattacks, warns DHS." *ABC News*, April 17. https://abcnews.go.com/US/emergency-services-target-cyberattacks-warns-dhs/story?id=109348647#:~:text=Calling%20911%20is%20meant%20to,multitude%20of%20dangerous%20ripple%20effects.

Lyngaas, Sean. 2024. "Cyberattacks are hitting water systems throughout US, Biden officials warn governors." *CNN | Politics*, March 19. https://www.cnn.com/2024/03/19/politics/cyberattacks-water-systems-us/index.html.

Michael Regan, Jake Sullivan. 2024. *Cyberattacks are Striking Water and Wastewater Systems.* Environmental Protection Agency, Washington, DC: The White House. https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf.

Microsoft Threat Intelligence. 2023. "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques." *Microsoft Security*, May 27. https://www.microsoft.com/en-

us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

Natter, Ari. 2024. "US Warns of Cyberattacks Against Water Systems Throughout Nation." *Bloomberg*, March 19. https://www.bloomberg.com/news/articles/2024-03-19/us-warns-of-cyberattacks-against-water-systems-throughout-nation?embedded-checkout=true.

Quillen, Alanna. 2024. "Cyberattacks on the rise this year, as Biden administration issues new warning about threat on water systems." *NBC Dallas Fort Worth*, March 29. https://www.nbcdfw.com/news/local/cyberattacks-pose-threat-on-water-systems/3501611/.

Waldman, Arielle. 2024. "U.S. agencies continue to observe Volt Typhoon intrusions." *TechTarget*, May 7. https://www.techtarget.com/searchsecurity/news/366583581/US-agencies-continue-to-observe-Volt-Typhoon-intrusions.

Walter, Jim. 2023. "Iran-Based Cyber Av3ngers Escalates Campaigns Against U.S. Critical Infrasctucture." *Sentinelone.com*, November 30. https://www.sentinelone.com/blog/iran-backed-cyber-av3ngers-escalates-campaigns-against-u-s-critical-infrastructure/.