A Tale of two Typhoons: properly Diagnosing Chinese Cyber Threats.
By Erica Lonergan and Michael Poznansky on the War on the Rocks website Warontherocks.com, Published on Feb 25, 2025.

A Summary Aired by KD5BJ

As we see in horror the terrible devastation brought by Hurricane Melissa, and as the hurricane season comes to a close, it is time to look at typhoons. And these typhoons can be as horrific but they are mad made, Chinese made to be clear, and attack our infrastructure and our communications.

In 2024 , Chinese cyber threat actors have gained access to important U.S. networks.

The most famous one is Volt Typhoon, which burrowed into U.S. critical infrastructure, potentially to preposition cyber assets in the event of a crisis or conflict with the United States, and Salt Typhoon, which penetrated multiple telecommunications networks to spy on Americans.

Volt Typhoon and Salt Typhoon share a few things in common starting with their name. But when it comes to operational and strategic objectives, however, these two "typhoons" represent fundamentally different kinds of threats.

Salt Typhoon, by all accounts, appears to be a classic — if somewhat breathtaking in scope — case of espionage. The intrusion, which entailed gaining access to unprecedented amounts of extremely granular information from some of America's largest telecommunications companies including Verizon and AT&T, was an intelligence bonanza for China.

According to major reports, hackers gained access to extremely high-value targets, including then President-elect Donald Trump's and Vice President-elect JD Vance's cell phones. Salt Typhoon had as target our National Security.

Volt Typhoon represents a different sort of breach entirely. U.S. officials, together with Five Eyes intelligence partners, described in early 2024 how Volt Typhoon "has been pre-positioning themselves on U.S. critical infrastructure organizations' networks to enable disruption or destruction of critical services in the event of increased geopolitical tensions and/or military conflict with the United States and its allies."

Then-director of the Cybersecurity and Infrastructure Security Agency, Jen Easterly, warned in Congressional testimony about how Volt Typhoon could "well endanger the lives of Americans here at home — through the disruption of our pipelines, the severing of our telecommunications, the pollution of our water facilities, the crippling of our transportation modes," and of course shutting down our grid in a future crisis.

For Salt Typhoon, the big challenge policymakers face is that while cyber deterrence in general is always difficult, it is especially tough to deter cyber espionage specifically. But in the case of Salt Typhoon, China has *already* captured sensitive information from its unauthorized access to U.S. telecommunications providers, and is likely acting on the intelligence, making deterrence for this particular operation moot.

Volt Typhoon is a different story. Unlike Salt Typhoon, where the benefits to China are effectively immediate from access to telecommunications networks, in this case, the actions the United States most wants to deter — disruptive or destructive cyber operations against critical infrastructure — have not yet taken place.

China is holding a capability in reserve, and its access is primarily valuable insofar as it gives China tools it can use later. This creates a window for deterrence. Several implications follow.

Most obviously, it means China is unlikely to deliberately activate its pre-positioned disruptive or destructive cyber capabilities unless there is a crisis or a war with the United States. As a result, to deter such cyber operations, the United States should primarily focus on deterring conflict with China — rather than narrowly concentrating on the cyber dimension of the threat.

And what if the United States fails to deter war? The question then becomes whether the *activation* of these exploits can be deterred in the event of conflict. To better understand this issue, we need to distinguish between counterforce versus countervalue targeting.

Counterforce in this instance refers to activation of Volt Typhoon exploits specifically oriented toward military bases, facilities, and other infrastructure that could impede effective military mobilization and operations.

Countervalue captures cyber operations aimed at civilian populations with the intention of disrupting daily life, sowing chaos, and causing pressure on American policymakers as a result.

If China ultimately believed the United States would fight for Taiwan directly, and Chinese leader Xi Jinping still decided to initiate a war, there is likely little that could be done to deter Volt Typhoon actors from trying to activate any available exploits against counterforce targets.

With direct fighting assumed, it is unclear what would prevent China from attempting to use all available tools to slow down the U.S. effort to defend Taiwan. The real solution, then, would be to focus on improving the resilience of the targets, actively removing malware, ensuring secondary and tertiary capabilities, and so on.

Deterring China from activating countervalue exploits is a bit more complex. One potential source of deterrence may simply be that China fears such disruptions would backfire.

While it is possible, according to one analyst, “the [United States] might refrain from aiding Taiwan in times of crisis for fear of domestic disruption,” it is equally plausible that major attacks on U.S. critical infrastructure could backfire and galvanize the American public behind a robust response. Another potential source of deterrence is “mutually assured disruption,” which National Security Advisor Waltz himself has alluded to.

There is little we can do as ARES for the salt Typhoon. But I firmly believe that we can make a difference in our community and county for Volt Typhoon. When the grid goes down, our phones will not work.

But our radios will. Unlike an EMP, our radios will not stop working, nor those of others. We must be aware, however, that everything involving the use of Internet will likely not work in this kind of circumstances.

We can talk to each other, other counties EMC or EMCs etc. That is why I love our team. We train, we do exercises, we have a very talented Tech Team that helps us with our equipment. I think our resolve to increase repeaters, involve GRMS, interoperability, etc. is right on target.

Building it can be challenging as it depends on others. And of course, the elephant in the room, it depends on funding, or lack of thereof, as grants tend to advance ham radio in general, not emergency related needs. Regardless, I think the effort is critical and worthwhile.

Thank y’all for all you do, and visitors listening to the net as well. Please join us. Together we can overcome these and other threats to build a more resilient community.

KD5BJ back to net

Link to the article is here.