# Day 3 – Volt Typhoon Threat Actor

COA: Disrupt power generation and electric transmission by mis-operation of operational technology devices.

Motivation: Disrupt and/or mis-operate power generation and electric transmission infrastructure to draw focus from the South China sea prior to further amplification of operations.

Storyline: U.S. intervention in the South China sea has decreased as a result of multiple ongoing conflicts in the region. The People’s Republic of China (PRC) is taking advantage of this opportunity by increasing its operations in the South China sea. U.S. Intelligence and news/media report that Chinese operations are likely to continue and intensify.

These increased cyber-attacks on U.S. critical infrastructure targets are intended to further reduce U.S. focus in the South China Sea prior to another significant surge in PRC activity in the South China Sea. The significant surge in PRC activity is the mobilization of PRC resources, conducting staging activities that are consistent with pre-invasion operations.

Specific Targets for Consideration:

* OT LAN (10.0.9.0/24)
  + PRO: Directly effects the power generation, transmission, and distribution
  + PRO: This network is a good candidate for persistence.
  + CON: This network is not an initial access candidate.
* Engineering LAN (10.0.8.0/24)
  + PRO: Consistent with COAs, motivation, and storyline. They are aiming to disrupt power
  + PRO: Can disrupt power generation, transmission, and distribution
  + PRO: Can access the OT LAN via the WireGuard VPN
  + PRO: Due to WireGuard VPN tunnel, this network is a favorable candidate for persistence.
  + CON: This network is unlikely to be an initial access candidate.
* Infra LAN (10.0.1.0/24)
  + PRO: Good candidate for persistence.
  + CON: Not along the path for courses of action.