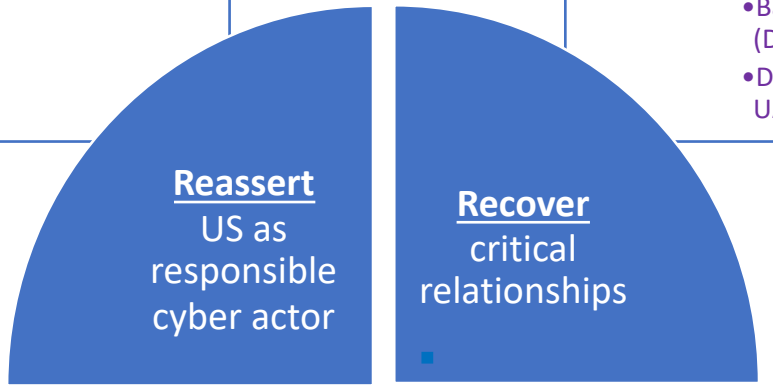
We are recommending a strategic response, grouped across four critical lines of effort – Reassert, Recover, Repair, and Restore.

SITREP

- Cyber incident at Ras Abu Fontas water desalination plant in Doha (21 Nov)
- DNI investigation confirms PENSIVEPENGUIN found at plant is USG persistent access tool to collect info on PLA infrastructure
- PENSIVEPENGUIN used by non-USG actor and proliferates globally
- Suspect in arrest following incident in Qatar is alleged US citizen

ASSESSMENT

- Vulnerabilities in US CNI unknown
- Moderate to high damage to relationships with allies
- Implications for US-Qatari relationship
- Incident likely perpetrated by non-state actor
- Chinese reputation damaged, opportunity for leverage



Reassert
- Engage with India as President of UNSC to establish cyber rules of the road for great powers (USUN, DoS)***

Recover
- Establish strategic Qatari water reserve (USAID)**
- Gulf cyber open-dialogue in Oman (DoS)**
- Back-channel with France (DoD)*
- Diplomatic messaging to UAE (DoS)*

Repair
- Public-private coordination (CISA, EPA)*
- Patching domestic networks (EPA)*
- #desalinatethenetwork info campaign (CISA)**
- Roll out Yuma patch to affected countries in Africa/Asia (CISA)**
- #dragonbugsbite bug bounty (NSA)**

Restore
- Request consular access to alleged US citizen (DoS)*
- Provide update on impact to USIC collection capabilities (DNI)**
- Conduct lessons learned wrt PENSIVEPENGUIN (CIA, FBI)***

*Immediate action
**Near-term action
***Long-term action

18 DECEMBER 2022