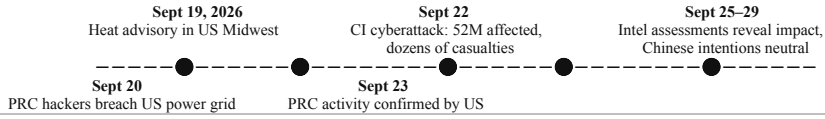
**TO:** Deputies Committee, National Security Council
**FROM:** Phish Finders – Amaury Dujardin, Arthur Muiru, Arnav Sahai, Tracy Zhang
**RE:** Recommendations Following the September 2026 Cyberattack on the U.S. Power Grid

**EXECUTIVE SUMMARY:**

On **September 20, 2026,** amid a record Midwest heatwave, a **PRC-linked cyberattack** disabled segments of the **U.S. power grid**, leaving 52 million Americans without electricity and causing dozens of civilian casualties. U.S. intelligence confirms state-sponsored intrusion into critical infrastructure near key military installations, likely part of a gray-zone reconnaissance campaign related to Taiwan. Although Beijing's intent appears non-escalatory, the incident exposes a growing PRC willingness to weaponize U.S. domestic vulnerabilities for strategic leverage.




**INITIAL ASSESSMENTS:**

**Short Term - Description** **Severity: High | Likelihood: Medium**

- **Should not go beyond three lines**

**Long Term - Geopolitical Power Shifts** **Severity: High | Likelihood: Medium**

- **The cyberattack could mark the beginning of the PRC's takeover of the South China Sea**, giving it control over the region, which generates trillions of dollars in annual economic value. The PRC could thus pressure Southeast Asian nations to acquiesce to its demands, severely denting the US's global influence.

**RECOMMENDATION: Pursue Option 2 - Defend & Attribute**

Option 2 best serves the White House's strategic objectives. Protects Americans. Punishes China. Leads Allies.

| OPTION 1 - Defend at Home | OPTION 2 - Defend & Attribute | OPTION 3 - Disrupt |
|---|---|---|
| • Complete digital forensics report: scope, impact, tactics used<br>• Containment and eradication of the adversary's access<br>• Intelligence sharing with allies, including Five Eyes<br>• Strengthen US CI through creation of US Cyber Force<br>• Diversify US energy resources | **Option 1 and:**<br>• Offer subsidized US cybersecurity services to allies abroad<br>• Attribute the attack and orchestrate collective diplomatic and legal response against the PRC:<br>• Formally request remedial action<br>• Pursue charges against identified perpetrators in concert with InterPol under the Computer Fraud and Abuse Act | Options 1, 2, and:<br>• Plan a counterstrike that disrupts the Great Firewall<br>• Target state media (i.e. *the Global Times*) and publish anti-PRC propaganda on their websites<br>• Economic sanctions |
| ✅ Short-term: De-escalates conflict with the PRC<br>✅ Long-term: Addresses major gaps in US CI<br>❌ US citizens may desire a proportional response<br>❌ Could invite the PRC to continue strikes on US CI | ✅ Strengthens US' image abroad and diminishes PRC's<br>✅ Rhetorical response weakens PRC counter options<br>❌ US citizens may still desire a proportional response | ✅ Creates no direct casualties but sends a responsive warning shot<br>✅ Incommmensurate attack that should not escalate situation<br>❌ Cuts short global campaign against the PRC in Option 2<br>❌ PRC may choose to escalate |