

TO: White House Cyber Response Group
FROM: Phish Finders - Amaury Dujardin, Arthur Muir, Arnab Sahai, Tracy Zhang
RE: Recommendations following the Cyber Attack on the Philippines' Telecom Networks

EXECUTIVE SUMMARY:
Cyberattacks targeting the Philippines during heightened tensions with the People's Republic of China (PRC) over activities in the South China Sea resulted in intermittent outages in mobile networks and disruptions to government websites. These incidents created public confusion, economic loss, and eroded confidence in the Philippines' digital infrastructure. Initial investigation reveals that likely PRC-sponsored threat actors exploited vulnerable Philippine digital infrastructure, raising concerns in the US about reliance on Chinese digital services in its critical infrastructure.

INITIAL ASSESSMENTS:

Short Term - Cyberattacks & Military Conflict

Severity: **High** | Likelihood: **Medium**

- The United States' intelligence indicates that state-sponsored Chinese cyber groups have infiltrated the US's critical infrastructure (CI). Further escalation could lead to cyberstrikes from the PRC, exposing the US' safety.

Long Term - Geopolitical Power Shifts

Severity: **High** | Likelihood: **High**

- 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 - A Measured Response

Option 2 reaffirms the US as a trusted global partner while not escalating tensions, providing immediate support that promotes our economic interests and ensures access to intelligence to strengthen global CI.

POLICY OPTIONS		
OPTION 1 - Minimal Reaction • Intelligence sharing between allies, the U.S. • Digital forensics report: scope, impact, tactics used, and whether attackers still have access. • Containment and eradicate the adversary's access • Strengthen U.S. cybersecurity defenses in both the private and public sectors. ✔ De-escalates conflict ✔ Improves the Philippines' CI ✘ Weakens international governance ✘ Weak response to threat actors	OPTION 2 - Measured Response Option 1 and: • Subsidized cybersecurity deal between the Philippines and U.S. companies • Spur cooperation between the Philippines, Vietnam, and Taiwan to maintain defenses around their EEZs • Avoid direct attribution of the attack to the PRC ✔ Further improvements to the Philippines CI ✔ Improves interoperability between the Philippines and the US ✘ Tensions with PRC ✘ Increased cost to the US Treasury	OPTION 3 - Counterstrikes Options 1, 2, and: • Take necessary measures to attribute the attack, likely to the PRC • Proportional counter-attacks • Economic sanctions • Cases and complaints with relevant int'l bodies ✔ Demonstrates strength and solidarity ✔ Signals new, tough strategy, acts as a deterrent ✘ Invites retaliation ✘ Leads to escalation, possibly to a military option