TO: National Security Council
FROM: Ghost in the Shellcode [W. DeSombre, M. Lee, E. Plankey, B. Saunders]
RE: Policy Options – Mitigating Effects of Global STANDINGPALM Incident

EXECUTIVE SUMMARY: The November cyber attack in Qatar likely originated from a U.S. exploit being discovered by an unknown party. Public Chinese attribution of the U.S. has caused international uproar. Opportunistic threat actors are using the now public vulnerability to cause global supply chain and infrastructure instability. To mitigate this incident's diplomatic and security impacts, we recommend **Baseline Actions** to protect U.S. critical infrastructure and the global economy, and **COA 1** to respond to key French and Qatari concerns while maintaining strategic cyber capabilities.

PRIMARY ASSESSMENTS

Global Critical Infrastructure Insecurity **[Severity: High | Likelihood: High | Timeline: Immediate]**

- Widespread ICS outages in Africa and Asia hurt the global supply chain and economy. **We do not know how many global/U.S. firms are still vulnerable, or how the exploit was discovered outside USG**.

Plummeting Global Trust **[Severity: High | Likelihood: High | Timeline: Medium Term]**

- USG's current international standing is low due to this incident: tensions are high with France, the EU, China, and Qatar. Any solely-USG headed initiative will likely be less effective and viewed with distrust.

STRATEGIC OBJECTIVES: Protect U.S. critical infrastructure, ensure resilience of the global economy, regain trust with U.S. allies, and prevent the sacrifice of strategic priorities in the cyber domain**.**

RECOMMENDATION: COA 1 – *RESPOND*

COA1 provides solutions for **domestic and global resiliency,** concrete steps to **engage France and Qatar**, and creates opportunities to **regain trust internationally without sacrificing capabilities**.

POLICY OPTIONS

BASELINE ACTIONS

- **State** translates Yuma patching guidance into 50+ African / Asian languages.
- **CISA** issues vulnerability guidance to check for Yuma.
- **DHS/CISA** engages private sector to develop an open-source enterprise scanner for Yuma software.
- **FBI** announces public investigation into domestic organizations leveraging STANDINGPALM.

✓ Reaffirms U.S. commitment to protection of domestic and global critical infrastructure.
✓ Does not decry or apologize for U.S. behavior.
✗ Does not repair damaged relationship with key allies.

COA 1 - RESPOND

BASELINE and:

- **FBI** launches parallel investigation into U.S. national who abetted the attack, requests collaboration with **Qatari LE**.
- **White House** reaches out to Macron to propose a joint Call to Action/Summit on Cyber Norms.
- **State** facilitates discussions with Qatari and European officials to bolster Qatari energy supply to Europe.

✓ Smooths tensions with France and Qatar without sacrificing intelligence capabilities.
✗ Does not address other European allies.

COA 2 – ENGAGE

BASELINE and:

- **DOJ** requests extradition of U.S. citizen implicated in Qatar attack.
- **NSA/FBI/CISA** publicly attributes Chinese ICS capability collected through separate "Defend Forward" operations.
- **State** provides $250M in funding for Joint Cyber Defense Collaboration for the Global South.

✓ Shows commitment to global security while also diverting attention.
✗ May be ineffective due to distrust in U.S. government.