SEAFARER CYBER INCIDENT UPDATE, GEORGETOWN STIA STINGERS

BLUF: Our recommended COAs clarify government priorities, call for a multi-organizational technical response to mitigate potential future attacks. and call for the U.S. to lead the international effort to re-establish normal international shipping activity.

Background: (ICOD: 0500Z 21MAR2020) Major ports around the Pacific Rim are experiencing technical difficulties with the SEAFARER software leading to massive backups and threatening shipping around vital chokepoints. The Automatic Identification System (AIS), is also experiencing malware which severely corrupts its data. Whether these two malware suites or attackers are related is currently unknown.

Policy Recommendations & Analysis:

Policy Alternatives & Analysis:

1. Objective: Establish high-level bilateral dialogue focused on threat information sharing, mitigate shipping bottle- neck, ensure safe navigation, and coordinate responses (Lead: State Department, i.e. applicable Diplomatic Missions. Timeline: five days to contact and establish coordination channels.)
   Recommendation: Immediately engage the most severely affected states including China, the Philippines, Malaysia, and Indonesia to clearly communicate the extent of damage, intended USG response, and (shareable) progress toward attribution and patching. (We remain willing to develop a multilateral framework in the long-term.)
   Key Risks: Risk the loss of classified sources and methods. Diplomacy always takes time and domestic political environments (esp. in China) complicates the successful execution of this approach.

2. Objective: Address the threat to AIS to prevent any at-sea collision or loss of life and minimize further disruption of international shipping lanes. (Lead: Federal Maritime Commission, domestic messaging, International Maritime Origination, international coordination. Timeline: 1-2 weeks)
   Recommendation: Ships immediately cease relying on AIS for navigation—AIS is primarily an identification system vice a navigation system (pursuant to the USCG Navigation Center for Excellence). The FMC and its sister organization at the UN, the IMO will disseminate this information to mariners and harbormasters and instruct them to rely on shipboard navigation equipment and V/UHF radio transmissions for hailing.
   Key Risks: The paramount risk to avoid is any maritime collisions—especially of large, difficult to maneuver, vessels such as oil or LNG supertankers, and especially in a choke point or port.

3. Objective: Redouble our effort to understand both the malware and the threat actor(s) and develop mitigations for the new threats. (Lead: DHS CISA with analytical support from NSA and USCYBERCOM. Timeline: patching, likely 10-30 days; attribution, 30-60 days—longer to gather evidence for a federal indictment.)
   Recommendation: The Cybersecurity & Infrastructure Security Agency (CISA) will lead the government effort, leveraging technical support from NSA and USCYBERCOM, to advance technical responses, build resilience, and deter future attacks. Furthermore, CISA will serve as the locus for private sector coordination to develop and disseminate patches, and work to attribute the attack. If the Department of Justice determines that bringing federal charges are realistic, DHS will support DoJ's evidentiary gathering.
   Key Risks: tremendous administrative burden testing CISA's ability to coordinate both across federal, state and local government and among multinational corporations, in a highly time-sensitive environment. Delays in development and rollout will have extremely high economic costs (billions per day).

Justification of Recommended Policy Response:

- These represent achievable short-, medium-, and long-term goals to address a rapidly evolving threat.
- Allows ships to continue to navigate shipping routes, and reduces growing bottleneck at affected ports.
- Builds cyber resilience and a multilateral framework to respond to cyber-attacks affecting U.S. partners