LEWIS UNIVERSITY FLYERS DECISION DOCUMENT JANUARY 16th 2020

EXECUTIVE SUMMARY

ISSUE: Domestic-cross agency actions and policy recommendations in response to public outcry regarding election integrity, international national security issues regarding cyber mercenaries, and ensuring the security of the US critical energy infrastructure.

RECOMMENDATION: Initially, cross-agency actions should be taken immediately in accordance with the National Cyber Incident Response Plan. Three policy options have been outlined in addition to these actions. **Following the Necessary Cross-Agency Actions, we recommend starting with Policy Option 1: International Statements and Resource Prioritization.**

NECESSARY CROSS-AGENCY ACTION:

- **DHS** takes the lead for **asset response** (according National Cyber Incident Response Plan)
- **DOJ** takes the lead for **investigative response through** the **FBI** and **centralized** agency **communication** with the **NCIJTF**
- **CISA** needs to **validate that states followed emergency response plans for voters** when power was cut as well as the procedures for handling delays were taken in this situation.
- FBI and DHS will work with State Law Enforcement to publicly address political violence within individual states regarding protests.
- **DOJ** through the **FBI** should investigate a sampling of social media posts across affected states to determine whether claims were made by foreign bots or disgruntled voters. Outcome of this will determine whether to proceed with a domestic or international investigation.
- **DOE** in conjunction with **DHS through CISA can explore long term critical infrastructure regulatory standards**, and the options of rolling back to analog for most critical infrastructure points in order to disable possibilities of remote attacks
- Instruct the **ODNI to validate the state actor identified in the Rabinara Group report** before action can be taken in response

INTERNATIONAL POLICY RESPONSES

OPTION 1: INTERNATIONAL STATEMENTS & RESOURCE PRIORITIZATION

- Internationally, the Secretary of State can condemn the use of cyber-mercenaries and signal further consequences in order to encourage deterrence.
- Attribution should be withheld until there is high confidence about nation-state actor sponsoring "Speedy Sloth" specified in the Rabinara Report.
- Appropriate resources should be provided to domestic agencies to support the mitigation process.

OPTION 2: ECONOMIC SANCTIONS AND ALLIED COOPERATION:

- The Office of Foreign Assets Control can impose economic sanctions on responsible attacking entities and backing actors ONLY after a subsequent investigation.
- The US can also reach out through diplomatic channels to allied nation-states, and ask for cooperation in authorizing these sanctions in order to create a unified stance against the use of cyber mercenaries.

OPTION 3: MAINTAINING DETERRENCE AND DIPLOMATIC DEFENSE:

- Secretary of Defense can instruct the DoD and CYBERCOM to initiate covert offense-based attacks against involved entities infrastructure once attribution is placed, if technical avenues exist.
- Demand Russian cooperation in U.S. investigation and cease cyber privateering actions, utilizing diplomatic ties as leverage.