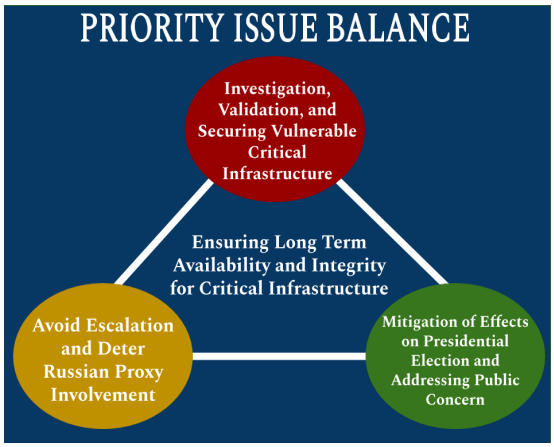
LEWIS UNIVERSITY FLYERS DECISION DOCUMENT JANUARY 16th 2020

EXECUTIVE SUMMARY



ISSUE: Points within the US critical energy infrastructure were brought down in at least 10 states during a potential attack from an unknown source on Election Day.

RECOMMENDATION: Four policy option response packages have been outlined. This acts in addition to cross-agency defenses that should be taken immediately. **We recommend starting with Option 2: Public Reassurance with Information Gathering and Cross Agency Actions.**

POLICY RESPONSES

Immediate cross-agency measures must be taken to protect critical infrastructure and national security interests according to the National Cyber Incident Response Plan. This involves actions taken by the following domestic agencies including: Department of Justice, Department of Homeland Security (CISA-ISD, ICS-CERT, EI and MS-ISAC), NSA, Department of Energy (CESER-CEDS, CESER-ISER, E-ISAC), and the National Cyber Investigative Joint Task Force (NCIJTF)

OPTION 1: TRANSPARENT PUBLIC OUTREACH & CYBER AGREEMENTS:

- Federal government can focus on public outreach regarding election issues and president can condemn the use of cyber mercenaries**.**
- Explore avenues of establishing a scheduled large-scale re-vote to keep the process trustworthy.
- Negotiate with Russia to share information and cease the recruitment of US 'cyber mercenaries'
- Develop an international agreement discouraging cyber attacks through private firms and 'mercenaries'
- *Lower Risk of Escalation, Lower Probability of Desired Outcome.*

OPTION 2: PUBLIC REASSURANCE WITH INFORMATION GATHERING & CROSS-AGENCY ACTIONS:

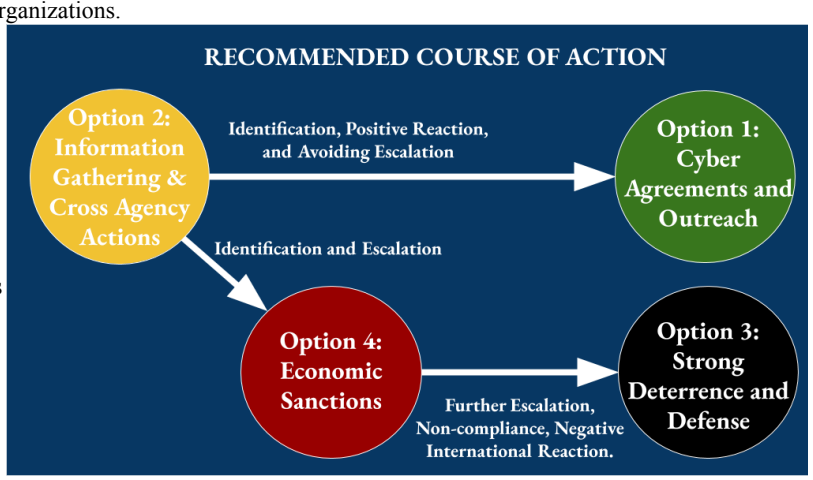
- **Cross-agency actions should immediately be taken in order to preserve the security of the country**.
- Domestic and international investigative agencies should **focus on gathering and validating intelligence.**
- **Resources should be provided to the DHS and DOE** to assure they can secure critical infrastructure for the long term.
- The President can **reassure the public through addresse**s regarding election issues, **stressing that integrity was maintained.**
- *Low Risk of Escalation, Medium Probability of Desired Outcome.*

OPTION 3: MAINTAINING DETERRENCE AND DIPLOMATIC DEFENSE:

- The President could instruct the DoD and CYBERCOM to **initiate offense-based attacks against entities involved in the attack**.
- **Demand Russian cooperation in U.S. investigation and cease cyber privateering actions**, **utilizing diplomatic ties** as leverage.
- *Medium/Medium-High Risk of Escalation, Medium Probability of Desired Outcome*

OPTION 4: STRONG ARM THROUGH ECONOMIC SANCTIONS AND COVERT ACTION:

- The **President can privately warn Russia about their recruitment and use of 'cyber mercenaries'** for privateering.
- The President may **also publicly signal consequences for the use of any private mercenaries**.
- If aggression does not cease, the President can invoke the IEEPA and **publically authorize sanctions on private cyber mercenary firms** including Sobornost **and individuals** linked to said organizations.
- Through US diplomatic channels, the **US could push allies to authorize these sanctions in order to create a standard against the use of 'cyber mercenaries**'
- *High Risk of Escalation, High Probability of Desired Outcome*



RECOMMENDATION

We recommend a dynamic nature of implementing these policies depending on how the situation escalates.