By the end of today’s meeting, our goal is to arrive at a shared understanding of success for this project.
• Purpose of today's kickoff is to review the proposed project plan on cyber risk. Our goal is to gather feedback on the following topics:
  – Project objectives and focal questions
  – Proposed analytic activities and deliverables
  – Collaboration and engagement with the AFRI team
  – Project Timeline
In answering these questions, the project will accomplish the following:

- Identify those states which are likely to serve as origin or transit countries for malicious cyber events.
- Develop a statistical model that will provide input to a development, diplomacy and defense framework for nation-state responsibility of cyber attacks.
- Guide US responses and focus resources required to establish robust systems of development, monitoring, controls, sanctions and defensive measures to ensure that cyberspace functions as a trusted and heavily defended environment that fosters cooperation, collaboration and commerce.

- How are cyber threats emerging from nation-states influenced by local economic, cultural, political and military factors?
- What do malicious cyber activities in those countries mean for U.S. interests globally?
- Is it possible to quantify those variables influencing a state's likelihood of being an origin or transit country for malicious cyber events?
### US Response Framework

<table>
<thead>
<tr>
<th>Range of State Activity</th>
<th>Development</th>
<th>Diplomacy</th>
<th>Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>State prohibited</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State prohibited but inadequate</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State ignored</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>State encouraged</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>State shaped</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>State coordinated</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>State ordered</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>State-rogue conducted</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>State executed</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>State integrated</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Methodology

- Panel data regression
  - Natural analysis with temporal and spatial data
  - Statistical evaluation of policies
  - Convert to a color coding

- Cluster analysis
  - Classic heat mapping tool
  - Emphasis on spatial correlation
  - Not useful for statistical evaluation
• Adapt a spatial panel data model in which 25 countries will serve as the units of analysis.

• While fifteen years is the objective, methodologies as well as data collected will change over time and may not be available. As a result, certain aspects of the study may require adjustments.

Data Sources

• Cultural
• Internet Usage and Online Habits
• Economic/Financial
• ICT Infrastructure
• Political
• Diplomacy and International Cooperation
• Military
• Law Enforcement and Rule of Law
• Technology
• Big Data, Other Non-traditional open sources
Products

- Statistical model for explaining malicious cyber activities
- Cyber risk map
  - Current
  - Projected
  - Hypothetical
- Findings will be disseminated through a cyber risk web portal, scholarly publications, issue briefs and technical briefs, distributed via mailing lists, email blasts, social networking websites, and blogs.
Possible Dependent Variables

- Botnets
  - C&C
  - Drones
- DDoS Attacks

Possible Explanatory Variables

- Cultural
- Internet Usage/Online Habits
- Economic/Financial
- ICT Infrastructure
- Political
- International Cooperation
- Military
- Law Enforcement
- Technology
Questions?