Abstract
China poses arguably the greatest national security threat to the United States. The uncertainty and lack of historical precedent for conflict in the cyber domain adds another dimension of complexity to this threat. The goal of our research was to analyze the relationship between the United States and China regarding Cyber Policy, using Game Theory simulations and the framework of the extensive form games to formally model conflict scenarios and to demonstrate the applicability of Game Theory to this great power dynamic.

Methods
1. Conduct thorough background study of applicable game theory information and strategy
2. Discuss the relationship between the US and China through an extensive form game considering pre-play signaling and a broad action space
3. Use python code to predict potential game scenarios and outcomes
4. Include parameters for learning and evolving strategies

Results
- Despite a lack of historical precedent in the cyber and national security domains, Game Theory allows us to generate a large set of possible behavioral sequences and empirically evaluate the possible behaviors.
- The image below depicts a series of potential actions and outcomes if the Chinese and the United States were to find themselves in conflict in the SCS. These scripts allow for policy planning and considerations regarding the economic, military, and political repercussions for different actions.

Future Work
- Continued work includes using these two Game Theory simulations and the framework of the extensive form game to evaluate equilibria, recommend best practices, and strategize methods for mitigating the risk of conflict.
- The application of reinforcement learning to this formalized model would create a dynamic and versatile product.

References and Acknowledgements
Larry Rudolph, Outside Advisor, MIT CSAIL, Two Sigma LLC.