Cyberwarfare : Longitudinal Trends and Effects on Foreign Policy

Pujan Paudel, Computer Engineering (ENG)

Pardee Center Summer Fellowship, Boston University

Research Questions

- How has the threat actor landscape evolved over the years?
- How has the threat motivation landscape evolved over the years?
- How has the threat categories landscape evolved over the years?
- Case Study : United States as Victims of Cyber Attacks
- Conventional Foreign Policy Actions in interactions between Rival Dyads
- Are conventional foreign policy actions effective in reducing severity of future attacks ?

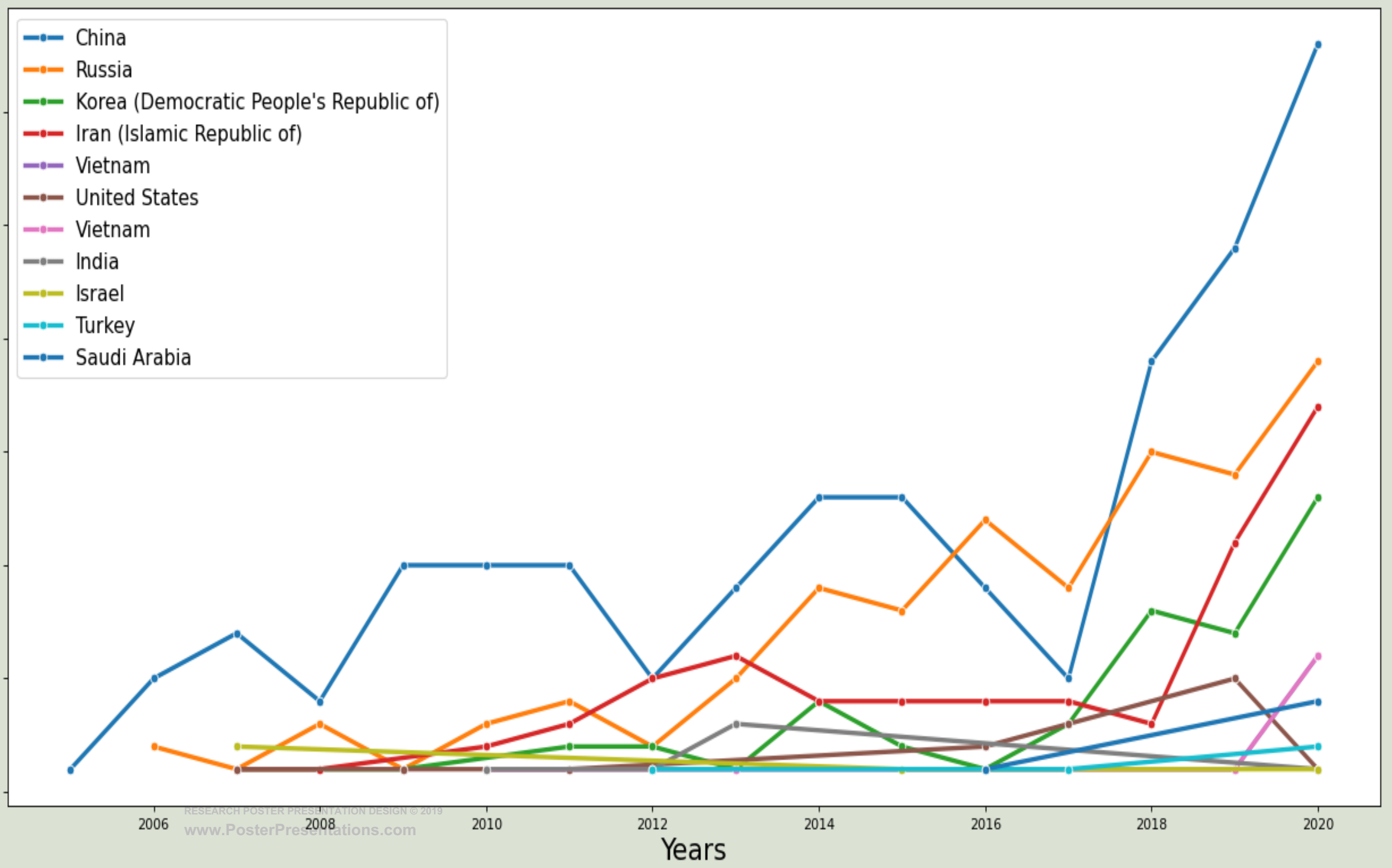
Background

- Attribution of Cyber Attacks is a complicated process
  - False flags
  - Shared code on cyber attacks
- Study : State-sponsored cyber attacks
  - Government press-releases
  - Reports from cybersecurity companies
  - Forensic analysis of cyber attacks confirming the affiliation of states

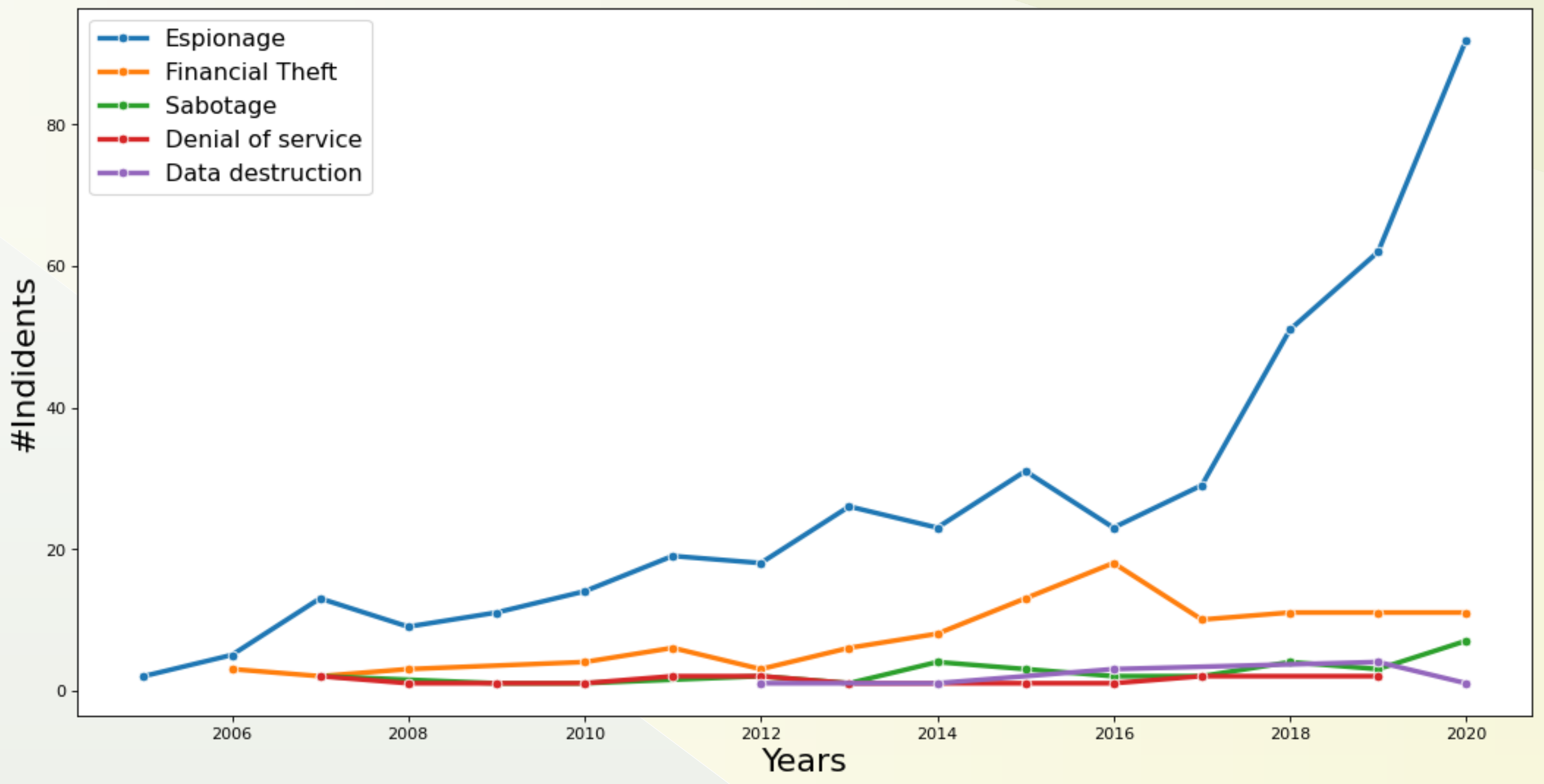
Dataset

- Compiled and aggregated data from three different data sources
- Normalized, Deduplicated entries across sources
- Comprehensive dataset of state-sponsored Cyber Attacks
- Conventional Foreign Policy Changes
  - Dyadic Cyber Incident and Campaign Dataset (DCID)
  - Integrated Crisis Early Warning System (ICEWS) events
  - Diplomatic, Economic, Military actions between rival dyads
- Sources:
  - Kaspersky Targeted Cyber Attacks Logbook
  - Council on Foreign Relations (CFR's) Cyber Operations Tracker
  - Threat Actor Encyclopedia by Thailand Computer Emergency Response Team

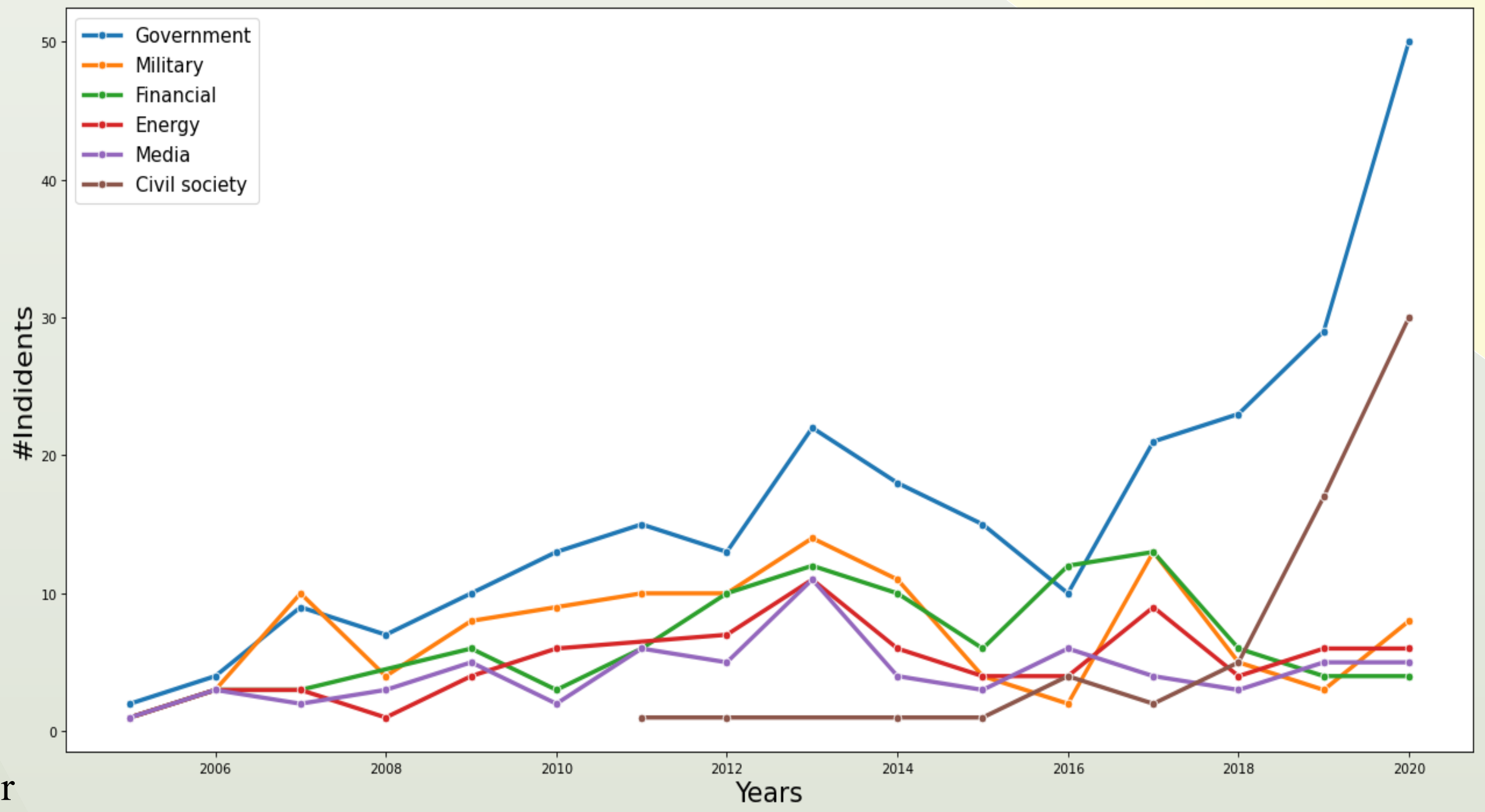
Threat Actor Evolution Over The Years



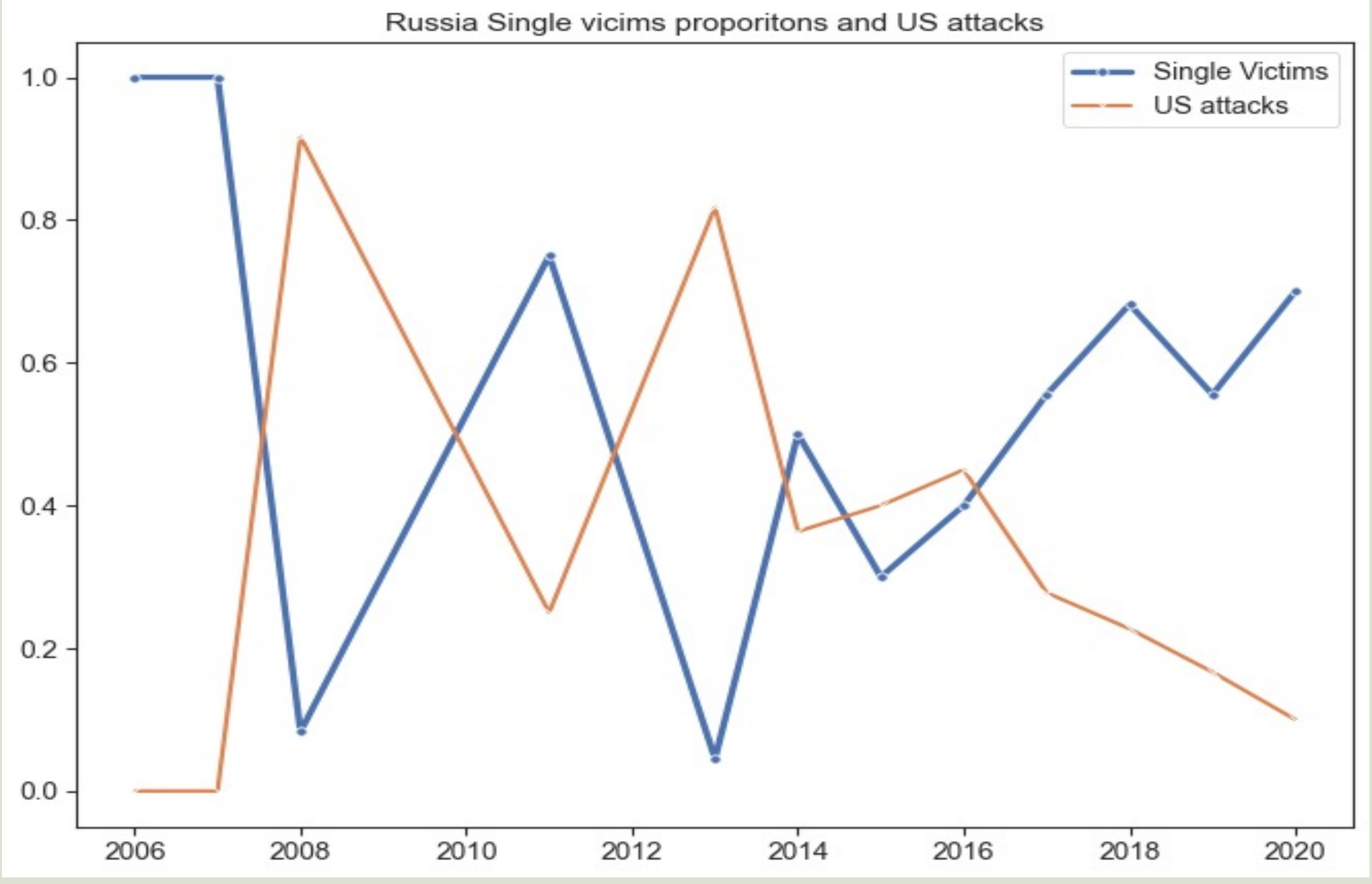
Threat Motivation Evolution Over The Years

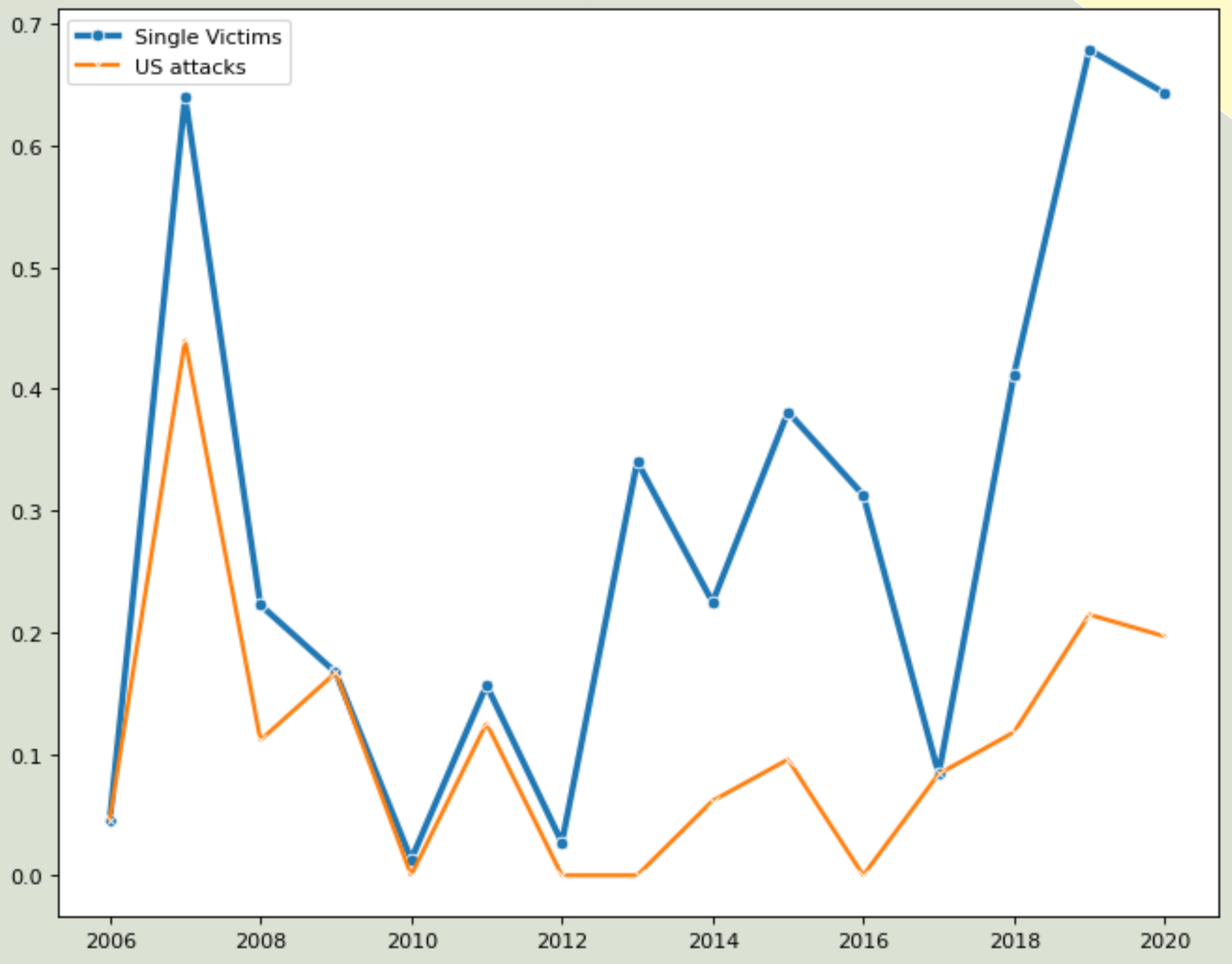


Threat Categories Over The Years



Russia and China : Singling out Attack Victims





Mean Cyber Severity Change As Effect of Policy Actions between Rival Dyads

Rivalry	Mean Cyber Severity Change
Russia-US	-0.073
Iran-US	0.25
Russia-Ukraine	-1.134
Iran-Israel	-0.325
China-US	-0.18

Mean Cyber Severity Change by Policy Actions

Policy Action	Mean Cyber Severity Change
Diplomatic Deny / Reject	-0.233
Economic Reduce	-0.090
Economic Threat	0.135
Economic Embargo / Sanction	0.259
Military Display	-0.111
Military Usage	-0.368

Takeaways

- Civil society sectors have been on the rise of targets.
  - Cyber-safety awareness and cyber-hygiene on the individual level
- Empirical analysis suggests us that intellectual agreement between China and US in 2015 to stop intellectual property theft was not effective after the Trump administration; largely due to the rhetoric of Trump administration against Beijing.
- China has been singling out cyber attacks against US
- With the flourishing of modern crypto-currency, financial theft could be the next big sector of cyber attacks after Espionage.
- Most of the conventional foreign policy actions have been impactful to some extent in helping decrease the volume of attacks in the future, which is a welcoming sign.
- Iran-US, Iran-Saudi Arabia, and China-Philippines have led to rather severe cyber attacks in the future.
  - Future work : What Went wrong between these countries ?
- Economic embargo and economic threat come out as the least effective foreign policy actions with regards to reduced severity of future attacks.
- While Military actions seem to be effective, diplomatic actions are also equally as effective in helping reduce the severity of future incidents.
- Policy Recommendation : Diplomatic foreign policy actions are the way to go !!

Acknowledgements

This project was supported by The Pardee Center Summer Fellowship Program. Special thanks to Dean Adil Najam, and John Prandato for guiding us through the summer fellowship program. Special thanks to my research advisor Dr. Gianluca Stringhini for his consistent mentoring throughout the project. Special thanks to Dr. Manjari Chatterjee Miller for her input and guidance throughout the project.

Contact