Visualizing the FiribiNome Social Botnet on Twitter:
Manipulating Social Influence through Networked Activity

Introductions
Social botnets are teams of software controlled online Twitter accounts designed to mimic human users and construct large networks of followers to promote specific online propagandists or websites. The bots exhibit a sophisticated strategy that remains undetected by Twitter. Their use to influence political opinion has been documented in the US, the MENA region, Ukraine, and Russia.

Botnet Behavior
Botnets in pervasive networks have been used to manipulate elections, but with the FiribiNome social botnet we observe a botnet that appears to promote specific accounts supportive to Jabhat al-Nusra. The FiribiNome social botnet has at least 120 accounts that all exhibit similar behavior. The bots tweet strings of mentions (see Figure 1), most of which are other members of the core bot network, along with the occasional mention of a high profile propagandist account or bot spokesmen account. Figures 2 and 3 both show the core bots have heavily weighted and highly dense edges to other core bots meaning they tweet often and frequently to other core bots. Their behavior appears to generate mentions of the propagandist accounts among their followers (see Figure 2), but we hypothesize that these behaviors could also generate followers for core bot accounts.

Key Findings
Although the purpose of the botnet’s structure and activity is not completely understood, we have the following hypotheses:

- Migrates followers from Propagandist accounts to core bot accounts
- Mention structure causes Twitter to place bot messages higher in followers’ Twitter feeds
- Generates more followers and attention for the botnet
- Migrates followers from Propagandist accounts to core bot accounts
- Mention structure causes Twitter to place bot messages higher in followers’ Twitter feeds

Visualization and Insight
One challenge in understanding the role of each account type within the Firibi Botnet and how the groups as a whole interact with each other is creating informative visualizations. We tried numerous network visualizations including force-directed, hierarchical, and box layouts. Each of these layouts were effective in grouping by account type, however the degree of edges produced by core bot members made understanding their relationship with other account types difficult. We found the hive plot to be an effective visualization to help hypothesize the function and purpose of the botnet. The plot preserves the separation of account types allowing one to understand the role of each group as a whole.

Future Research

- Measure the diffusion of the d3ua.org throughout the community
- Analyze similar bot structures found in other detected extremist communities
- Incorporate Natural Language Processing to inform detection strategies
- Gain proficiency in R and Python
- Understand how to utilize Natural Language Processing techniques to interpret social media activity in East Asia.