



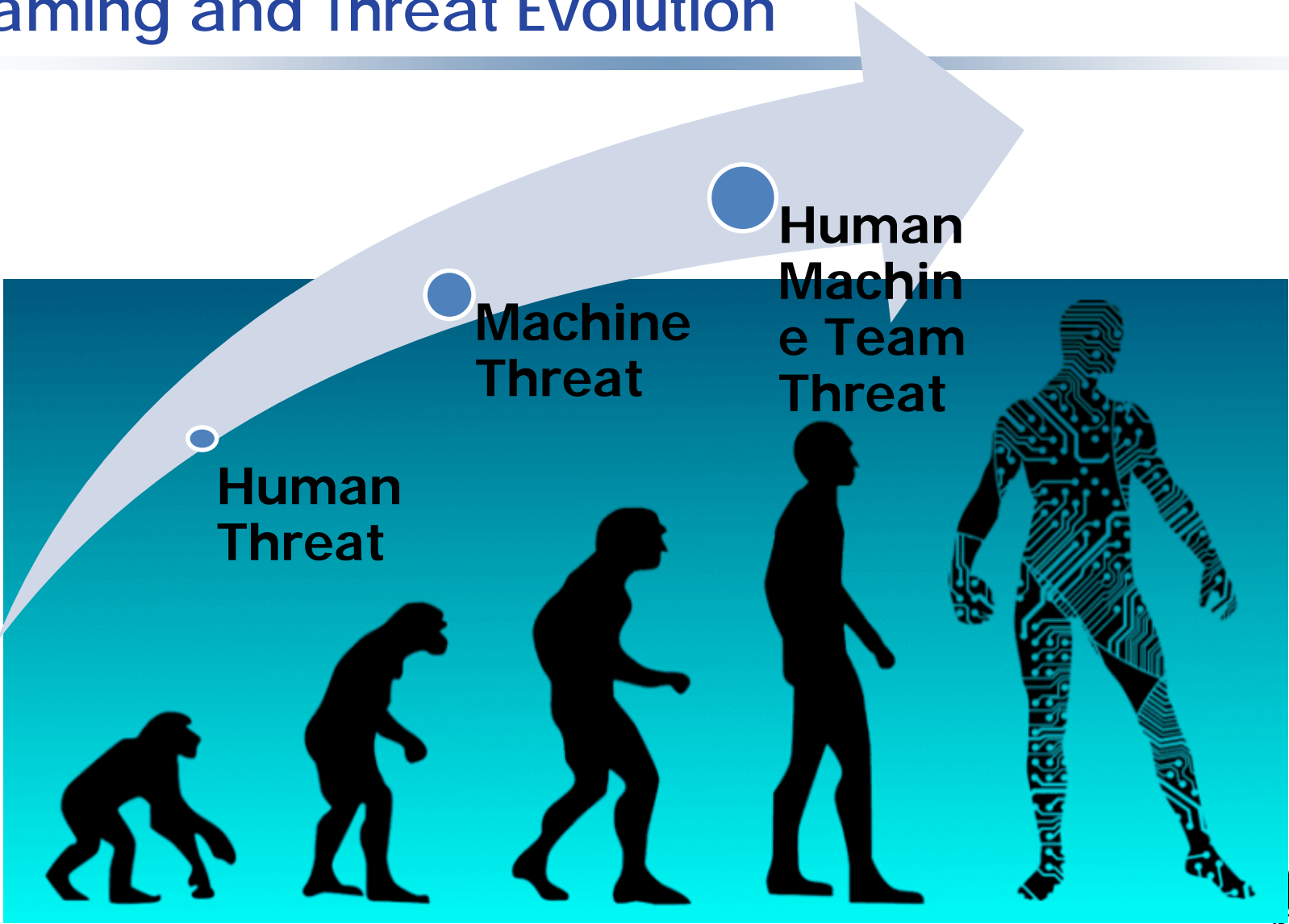
# *Human Threats versus Machine Threats in Cyber Security*

Kathleen M. Carley

# Social Cyber-Security

- the science to characterize, understand, and forecast **cyber-mediated** changes in human behavior, social, cultural and political outcomes  
*and*
- the engineering to build the cyber-infrastructure needed for **society** to persist in its essential character in a **cyber-mediated** information environment under changing conditions, actual or imminent social cyber-threats

# Teaming and Threat Evolution



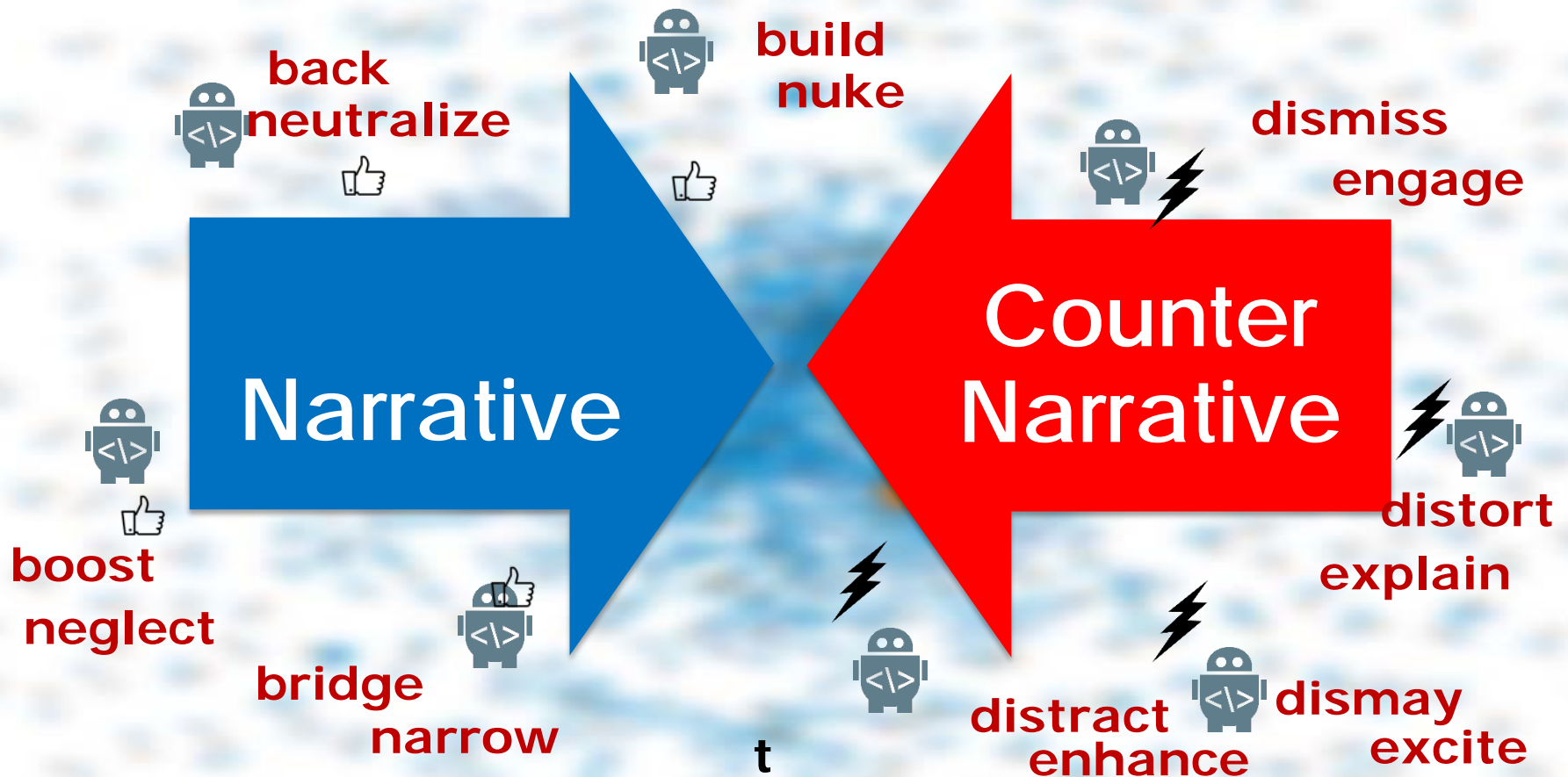
# What is Manipulatable

Posts, narratives  
 --- features of these  
 affect, emotional cues,  
 presence of memes, images,  
 font, cohesiveness ...



Actors, groups  
 --- features of these  
 network structure, position  
 of opinion leader, interaction  
 between groups ...

# The Information Environment

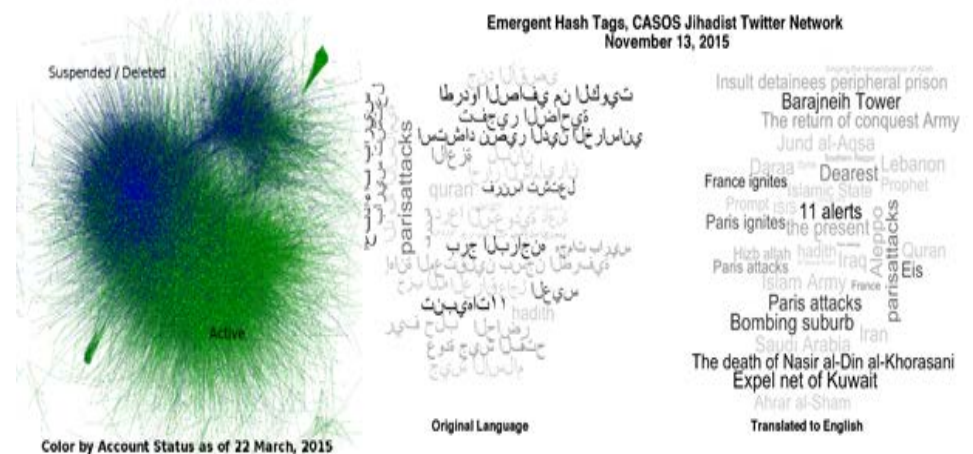


Bots/trolls are force multipliers that spread narrative and attack the counter narrative

# Echo Chamber, Bots and Manipulation

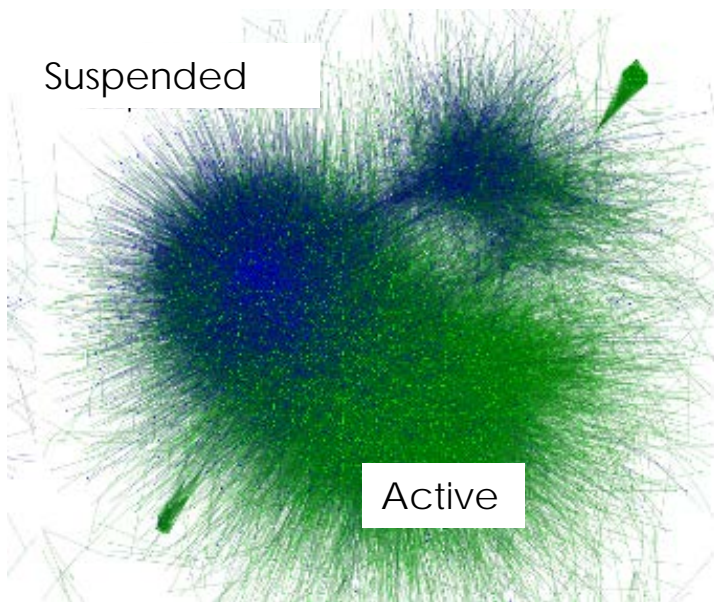
- A group that exhibits high connectivity in the community and content space
- This high level of connectivity leads to:

- a lack of objectivity
- a focus on common stories
- a sense of sharing
- suspicion or hostility to newcomers with different narratives
- rapid interaction with others with similar narratives.

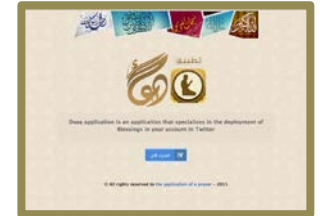
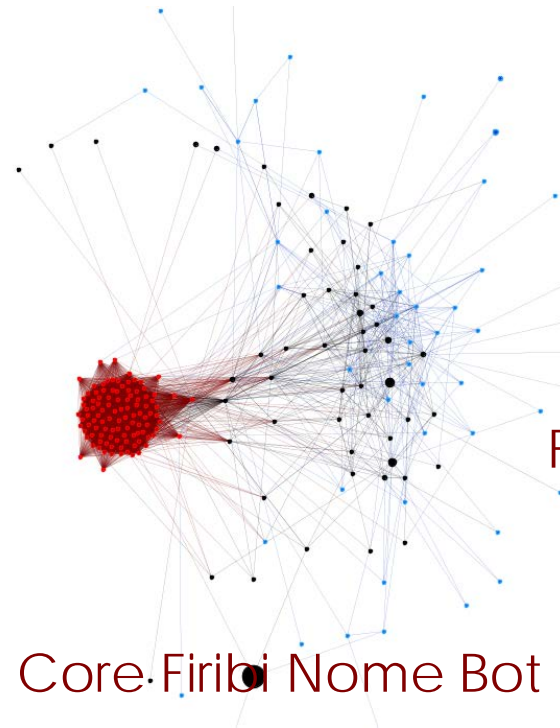


# Social Influence Bots Can Manipulate Topic-Groups

Syria Focused Extremist Topic Group  
"Dense Community"



Firibi Benefactorbbbbbb



App Sign Up, solicits donations for children of Syria

Firibi Follower





## B.E.N.D. & Firibi Nome

**Build** – Firibi Nome bot @mentioned each other thus creating a group

**Back** – Firibi Nome bots followed Imam increasing his perceived level of influence

**Bridge** – This bridged a connection between the Imam's topic group and the Firibi Nome's group

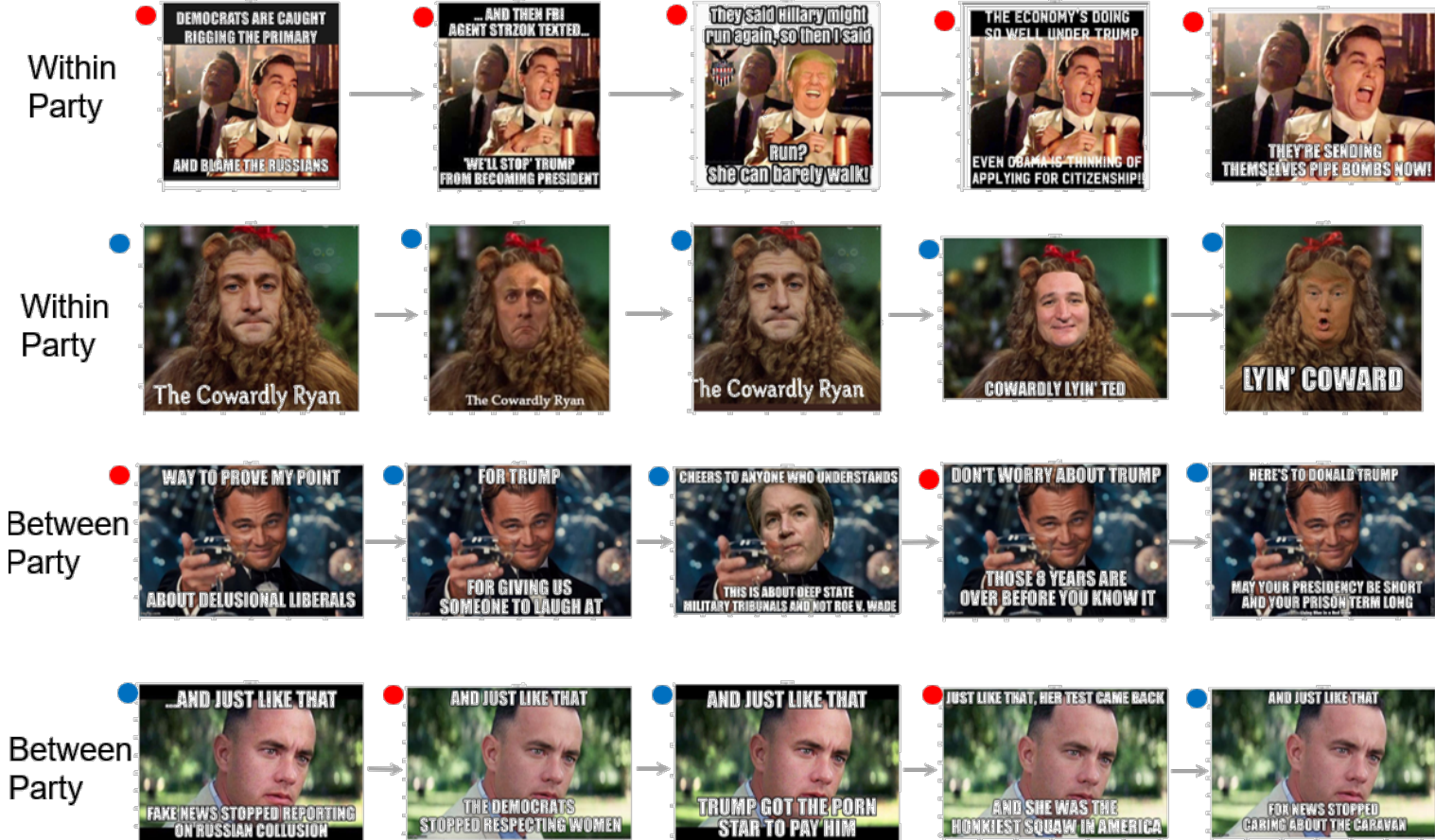
**Dismay** – Messages were sent about needs of children of Syria

**Back** – Messages were sent directing people to charity cite for children of Syria



# Mememes Track Political Debates

## Political Conversations with Memes



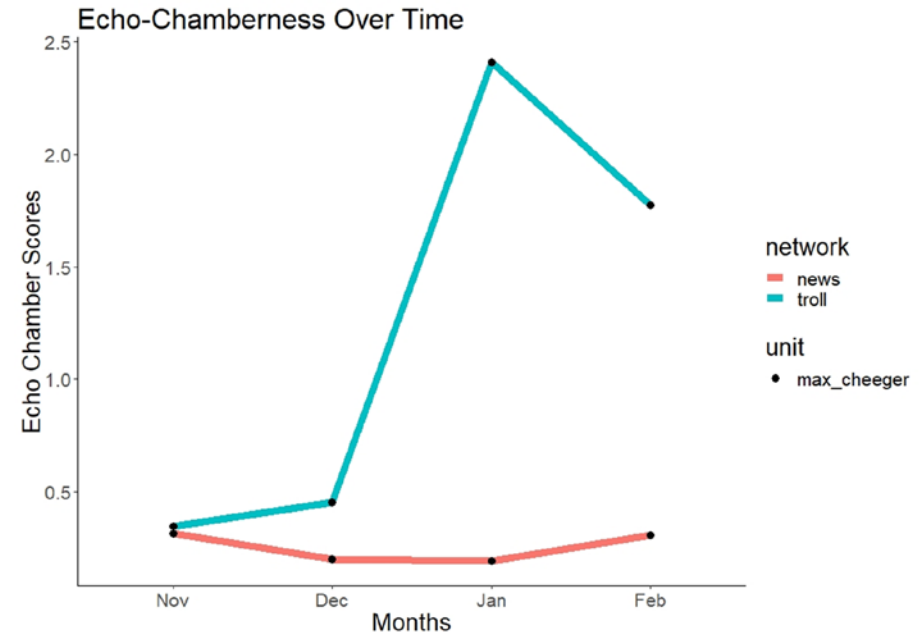
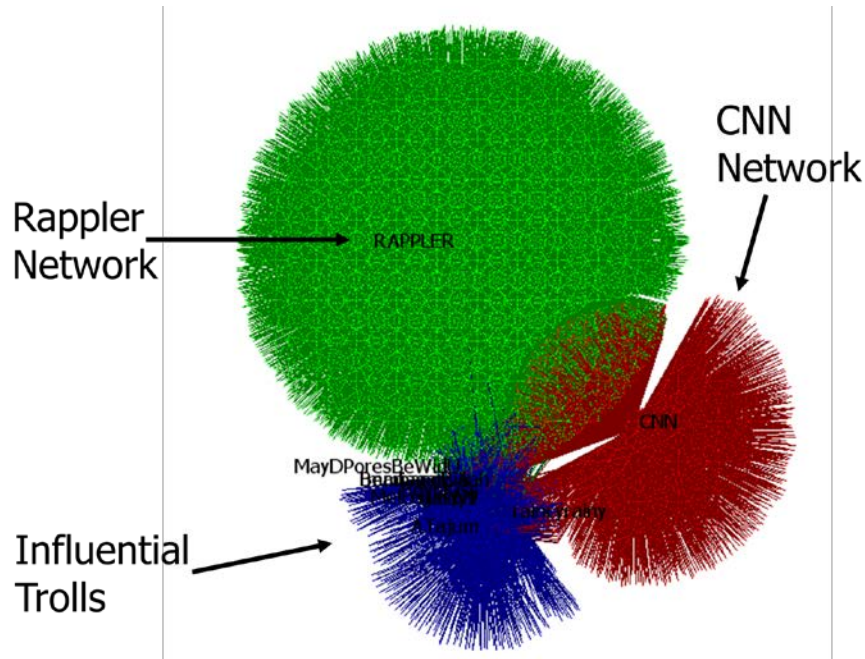
● Originating from the Left ● Originating from the Right ○ Origin unknown



# Chinese cautious approach to memes



# 2019 Philippine Elections



- News networks contain **mainstream election discourse** while troll networks highlight **partisan election discourse**.
- News networks feature **open discussions among general public** while troll networks are **denser and more echo chamber-like**.
- Troll networks start similar to news, grow to **8x as echo-chamber-like**.

# Trolls spreading Disinformation

- Media and human rights organizations are working together to oust the Duterte regime
- Cheating happening during overseas voting
- The media is censoring any Facebook comments that are against the opposition slate in the elections
- Only members of opposition party (Liberal Party) have multi-billion peso scams linked to their name
- Opposition candidate Mar Roxas urges citizens to "suffer" during water crisis
- Administration-backed candidate Imee Marcos is a graduate of Princeton University and the University of the Philippines College of Law
- Duterte aircraft drove off Chinese vessels from islands in West Philippine / South China Sea
- Previous administration sold the country to China
- Previous administration (Aquino) stole gold from the Philippines
- Chinese ships attacked Philippine ships

# Bots Trolls Cyborgs Exploit Technology and Social Cognition

- Technology
  - Scroll through technology
    - Frequent or repeated at top
    - Infrequent at bottom
  - Prioritization
    - Which followers get messages
    - Which topics & actors get recommended
    - Appears to take into account group density and opinion leaders
  - Abandoned accounts
    - Re-purposed
- Social Cognition
  - Apparent consensus
    - relying on generalized other
  - Create groups – us/them
  - Stereotype
  - Social inference
    - from individual to group
  - Tie utilization
    - Weak ties for news
    - Strong ties for controversy
- Cognition
  - Escalation of commitment
  - Confirmation bias
  - Intimidation

# Human and Machine Characteristics

- Human
  - Time, location and group constrained
  - Cognitive limited
  - Social cognition
  - Adaptive
  - Continuous learning
- Machine
  - Require training data
  - Biased by data
  - Fixed response
  - Treat tomorrow like today
  - Fast, easily duplicated

# Key Ideas

- Social Cyber-Security Arms Race
  - Cognitive security is a small part
- Technologies need to better take into account social cognition and true social networks
- Human threat
  - Adaptiveness
  - Deep understanding
- Machine threats in isolation
  - Scale
  - Speed
  - Geographic spread
  - Mimickry
- Human Machine Team threats
  - Hijacked teams

- <https://sites.google.com/view/social-cybersec//>
- <http://www.casos.cs.cmu.edu/>
- kathleen.carley@cs.cmu.edu