Social Cyber-Security Dynamics

Kathleen M. Carley
Kathleen.carley@cs.cmu.edu

All Metrics and Visualization capabilities are in ORA-PRO

Netanomics

Carnegie Mellon ISR institute for SOFTWARE RESEARCH

Social Cyber-Security

- the science to characterize, understand, and forecast **cyber-mediated** changes in human behavior, social, cultural and political outcomes

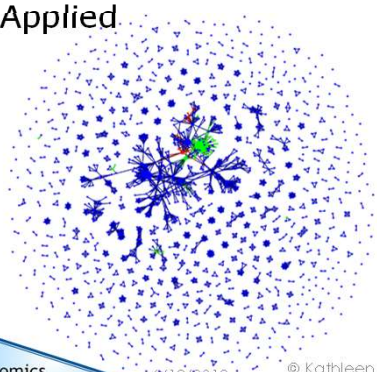
and

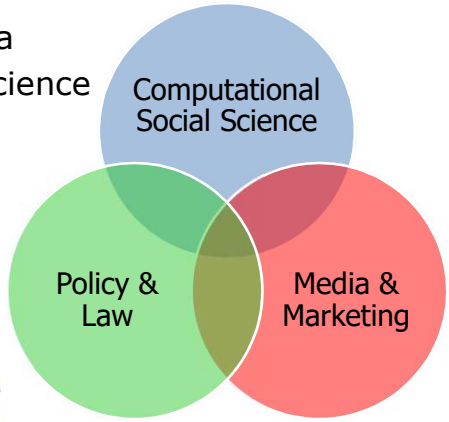
- the engineering to build the cyber-infrastructure needed for **society** to persist in its essential character in a **cyber-mediated** information environment under changing conditions, actual or imminent social cyber-threats

© Kathleen M. Carley, CASOS, ISR, SCS, CMU

Social Cyber-Security Characteristics

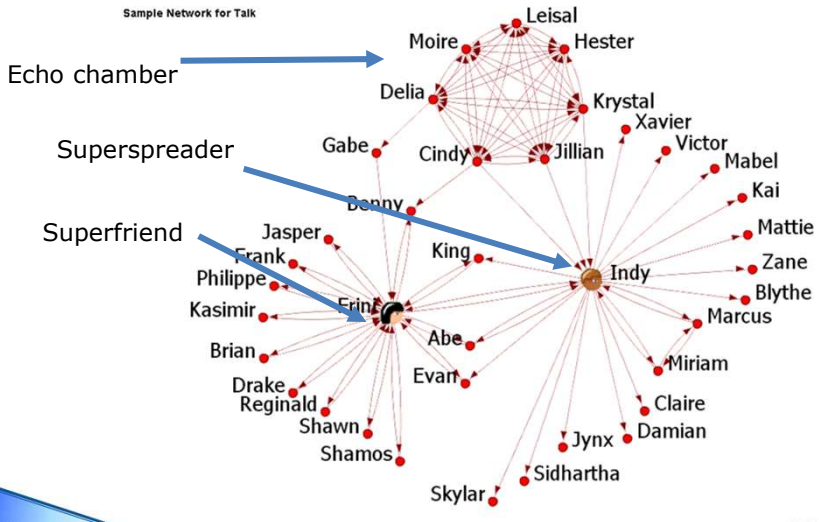
- Emerging scientific area
- Computational social science
  - Multi-disciplinary
- Multi-methodological
- Applied





© Kathleen M. Carley, CASOS, ISR, SCS, CMU

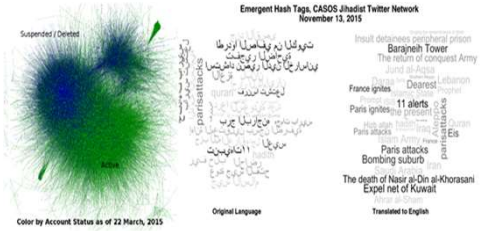
Social Media is About Networks



Copyright © Kathleen M. Carley 2019

Echo Chamber

- 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.



 Copyright © Kathleen M. Carley 2019

Traditional Information Warfare

- Dismiss
  - Belittle what is being said
- Distort
  - Twist the facts
- Dismay
  - Create fear inducing narratives
- Distract
  - Create or support a very different narrative

 Copyright © Kathleen M. Carley 2019

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 …

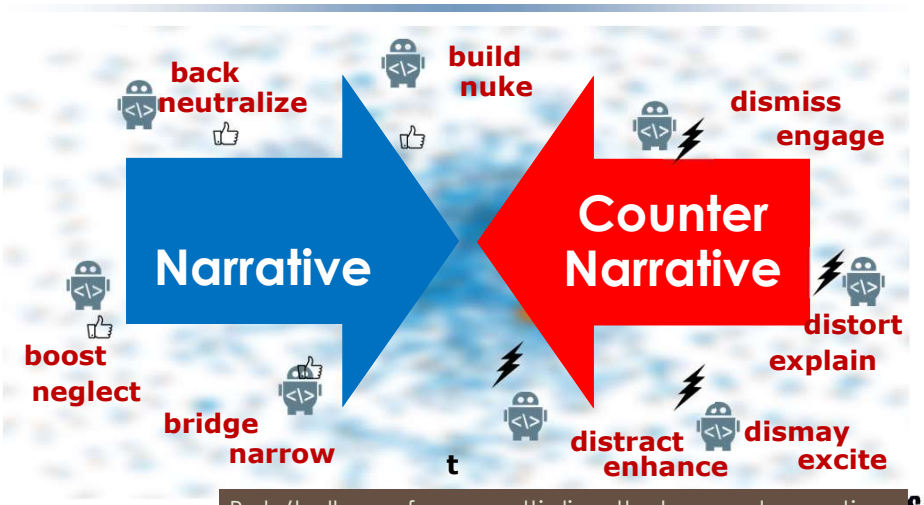
 Copyright © Kathleen M. Carley 2019

Key Findings

- Technology exploits
  - Manipulate privacy preserving schemes to enable multiple personas by same actor, or to increase trolls
  - Manipulate prioritization or ranking schemes
  - Manipulate timing and repetition features
  - Manipulate cross media linkages
- Social cognitive manipulations
  - Create appearance of larger or smaller group
  - Alter opinion leader status
  - Create appearance of consensus
  - Create appearance of multi-point confirmation
  - Alter cohesion
- General manipulations
  - Increase speed, scale, frequency, trending, send stories, repeat stories, increase modality

 Copyright © Kathleen M. Carley 2019

The Information Environment



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

Copyright © Kathleen M. Carley 2019

Positive

Negative

Excite Dismay
Trident Juncture PR with Russian

[redacted]

Dismay

Positive

Build

actions that create a group or the appearance of a group

Negative

Nuke

actions that lead to a group being dismantled

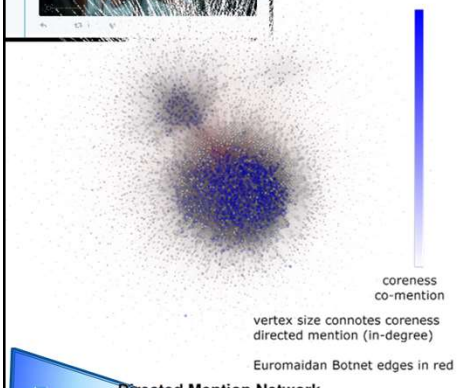
Netanomics 6/12/2019

© Kathleen M. Carley CASOS CMU, Netanomics

CASOS Carnegie Mellon

Positive

Build



Directed Mention Network

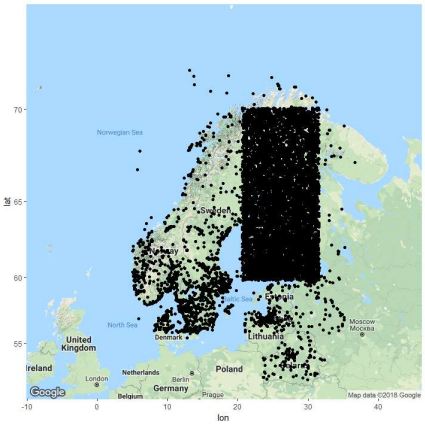
Netanomics 6/12/2019

© Kathleen M. Carley CASOS CMU, Netanomics

Negative

Nuke

Twitter Geo-Fence



CASOS Carnegie Mellon

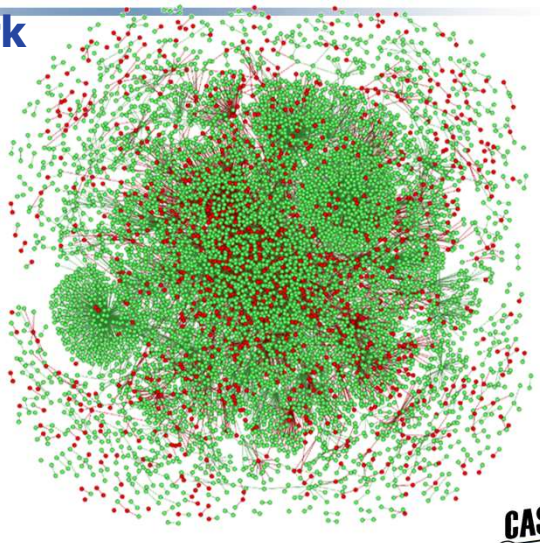
Tools of BEND

- BEND information maneuvers use diverse tactics and tools to exploit social media technology and so manipulate community and content
- Tools
  - Content focused
    - Memes
    - CUES
    - Images/videos
  - Community focused
    - Trolls
    - Bots
    - Cyborgs

© Kathleen M. Carley CASOS CMU, Netanomics

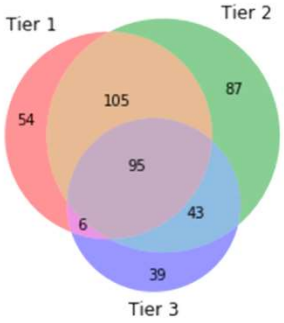
Bots in Network

Colored red if it has bot characteristics

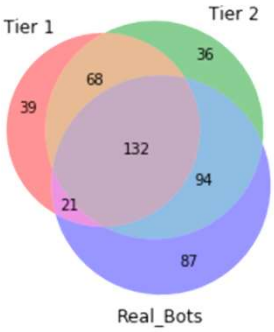


Copyright © Kathleen M. Carley 2019

Not All Bot Detectors Agree



(a) Predicted Bots (Tier 1, 2, & 3)

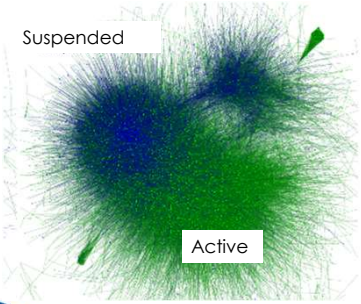


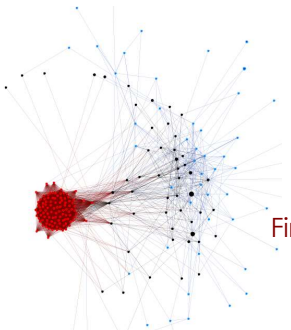
(b) Predicted Bots (Tier 1 & 2) with Real Labeled Bots

Copyright © Kathleen M. Carley 2019

Social Influence Bots Can Manipulate Topic-Groups

Syria Focused Extremist Topic Group "Dense Community"





Core Firibi Nome Bot

Firibi Benefactorbbbbb

App Sign Up, solicits donations for children of Syria

Firibi Follower

Copyright © Kathleen M. Carley CASOS CMU Netanomics

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

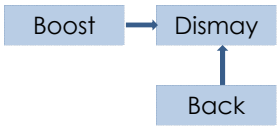
Back – Messages were sent directing people to charity cite for children of Syria

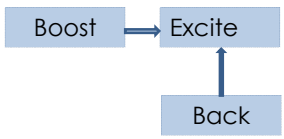
Copyright © Kathleen M. Carley 2019

Actions → Maneuvers → Goals

Strategic Goal

Russia vis NATO - Goal: Divide and Conquer



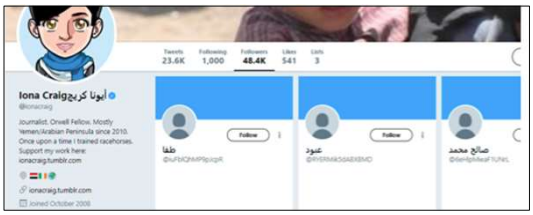


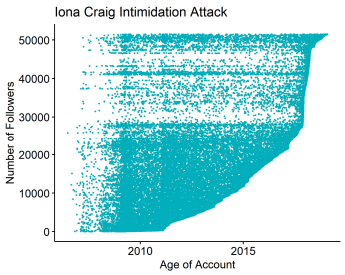
Used CUES Memes Images Cyborgs

© Kathleen M. Carley, CASOS, ISR, SCS, CMU

Bot Intimidation Operation

For the l 8-9 months, a determined actor has conducted an intimidation attack against Iona Craig, an Irish free lance journalist reporting on the conflict in Yemen [40]

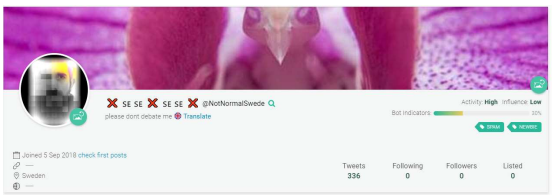


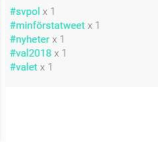


- Numerous random accounts follow her account every day, some with disturbing profile images.
- As of 6 June 2018, our Tier 0 algorithm showed that 18,800 of her followers had bot-like screen names.

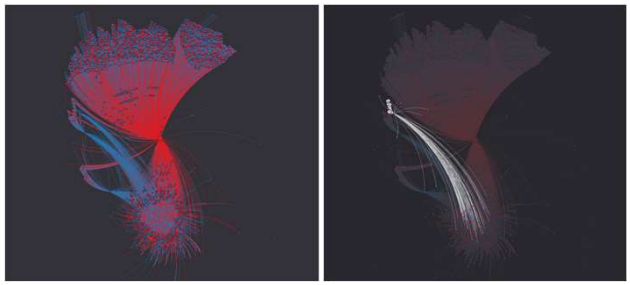
Nuke

Disinformation Maneuvers





Bridge



More than "fake news"

Information Campaign Lines of Effort

Present Russian Strength/Unity	
Weaken EU and NATO	
Polarize American Society	
Isolate Israel	

Memes Summarize Messaging

Overall

Pattern	
Bots as secondary	yes
Cultural ethos mission groups and disinformation from/to them	Harder to disrupt
Calling out	Yes – direct lie
Calling out	No - mission
Satire	Yes – direct lie
Disinformation as positive action	Spreads further
Half life general or direct lie disinformation	short
Half life of mission driven disinformation	Much longer

Copyright © Kathleen M. Carley 2019

Used in the Russian Disinformation Campaign

- Twitter
- Facebook
- Instagram
- Youtube
- Pinterest
- Tumblr
- Paypal
- Medium
- Reddit
- Gab

These were the core of the IRA campaign, and had the greatest impact

These seven were used to a lesser extent, but may provide interesting insights. Note that disinformation on these platforms is largely unexplored

https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep-tactics-evolved/
https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf
https://www.businessinsider.com/all-social-apps-russian-trolls-used-spread-disinformation-2018-12#vine-7

Challenge: Data Control & Management

- Data is not free and open
  - Providers dictate who can do what kind of science
- Data is often only a sample
  - Biases are often not known nor accounted for
- Data is not necessarily preserved
  - Replication is difficult if not impossible
- Data is not fully sharable
  - Reuse is limited
- Data production is time variant
  - Data providers change what is stored or collected
- Policies are out-of-sync with technology & science
  - Often not possible to collect the data needed to answer the policy question

© Kathleen M. Carley, CASOS, ISR, SCS, CMU

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

Two of many Related papers

- David M. Beskow and Kathleen M. Carley, 2019, Social Cybersecurity: An Emerging National Security Requirement, Military Review, March-April2019 – see https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b
- Kathleen M. Carley, Guido Cervone, Nitin Agarwal, Huan Liu, 2018, "Social Cyber-Security," In Proceedings of the International Conference SBP-BRiMS 2018, Halil Bisgin, Ayaz Hyder, Chris Dancy, and Robert Thomson (Eds.) July 10-13, 2018 Washington DC, Springer.

Copyright © Kathleen M. Carley 2019