Discovering Deception in Online Cybersecurity Discourse:

Using Social Media to Enable Effective Insider Risk Management

Mr. Luke Osterritter

losterritter@sei.cmu.edu

Document Markings

DM22-0551

Who We Are

Carnegie Mellon University
Software Engineering Institute

Carnegie Mellon University

- Pioneering discoveries that enrich the lives of people on a global scale
- Turning disruptive ideas into success through leading-edge research

Software Engineering Institute

- Bringing innovation to the U.S. government
- Researching software engineering, cybersecurity, and artificial intelligence

CERT Division

- Giving birth to modern cybersecurity
- Strengthening the resilience of systems and networks

C-InT SBS 2022 summit

Why is disinformation an insider risk problem?

- **BLUF** – adversaries can exploit and recruit insiders by way of mis-, dis-, and malinformation

One possible example:

- Theory of psychological **reactance** - "an unpleasant motivational arousal that emerges when people experience a threat to or loss of their free behaviors. It serves as a motivator to restore one's freedom." (Steindl et al. 2015)
- Individuals experiencing reactance as a result of actions or perceived actions of an organization may engage in organizational deviance.
- Such individuals may now be susceptible to **influence** from **adversarial entities** seeking to harm the organizations that the individual is a member of.

- Possible triggers
  - Office requirement
  - Vaccination reqs.
  - Extremists ideologies

From Insider Threat to Insider Risk

What is an “Insider Threat”?

- Malicious Insider
  - a current or former employee, contractor, or business partner who meets the following criteria:
    - has or had authorized access to an organization’s network, system, or data
    - has intentionally exceeded or intentionally used that access in a manner that negatively affected the **confidentiality, integrity,** or **availability** of the organization’s information or information systems
- Can also be inadvertent (non-malicious)

From Insider Threat to Insider Risk

- **Insider Threat**: Insider threat for an organization is the potential for an insider to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

- **Insider Risk:** Insider risk is the potential for loss associated with the realization of an insider threat.

As a discipline, we are moving away from a purely threat hunting mindset to one of risk management.

Insider Risk and External Threat

- Insider risk is unique in organizational security in that the potential threat agents play **fundamental roles** in accomplishing the organization's mission.

- Insider goodwill is **essential** to both keeping intentional insider risk to a minimum and ensuring organizational success generally.

- External adversaries can potentially use mis- dis- and malinformation with coordinated **information maneuver campaigns** to target trusted insider.

Mis- Dis- and Malinformation

What does “disinformation” mean?

Untangling the Terms

DISINFORMATION

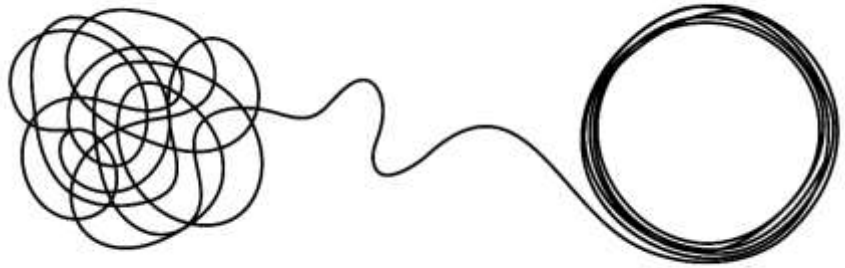
Information that is false and spread specifically by those who DO know it's not true.

MISINFORMATION

Information that is false but spread by those who DON'T know it's not true.

MALINFORMATION

Information that is based on fact but is spread – out of context – by people intending to mislead or cause harm.



Source:
IDeaS Center, CMU

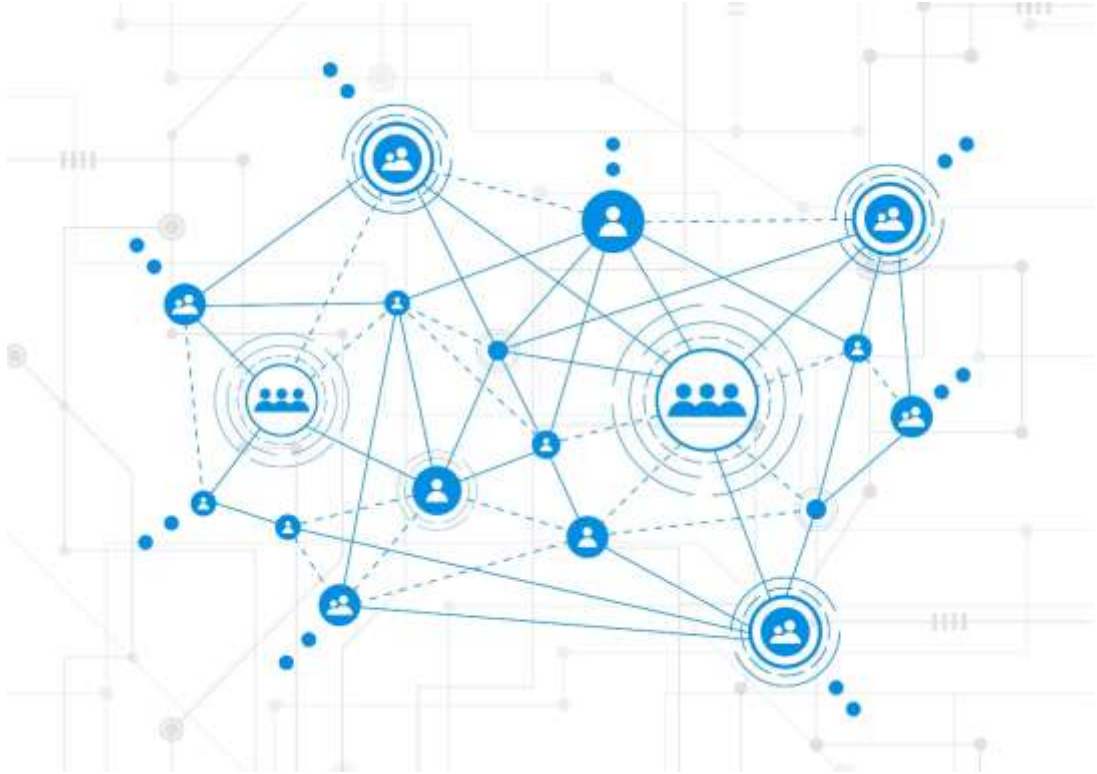
Why are disinformation, misinformation, and malinformation spread?

- Money
- Boredom
- Politics
- Disrupt society
- Reduce the voice of marginalized groups
- Building community

Source:
IDeaS Center, CMU

How does disinformation, misinformation, and malinformation spread?

- Bots
- Trolls
- Bogus news outlets
  - “Pink slime”
- Your family
- Your friends
- Me
- You!



Source:
IDeaS Center, CMU

Cybersecurity and Social Cybersecurity

- A scientific discipline to help us recognize and understand what's happening to us online and be able to see it coming

- Figuring out how to build policy and tech that protects society from social cyber threats

- **CYBERSECURITY**
  - Hacking machines
  - Harming confidentiality
  - Compromising data integrity and availability

- **SOCIAL CYBERSECURITY**
  - Hacking people
  - Capturing hearts and minds

Source:
IDeaS Center, CMU

Conversations around Insider Threat in Public Forums

C-InT SBS 2022 summit

Conversations around Insider Threat

- Why look at public conversation? Unlikely to find any insider threats…
- …but, there may be actors trying to shape the conversation to their own ends – corporations, nation-states, etc.
- Understanding the conversation will lead to informed research
  - Wisdom of the crowd
  - Data for computational modeling
- **Research question**: Can network analytical techniques be used to discover the nature of public conversations around insider threat and related organizational threats?
  - Gain **situational awareness** around public discourse

Source:
IDeaS Center, CMU

Collection Methods

- Use Python package twarc to retrieve tweets from Twitter Search API V1 based on hashtag query
- Tweets collected between March 27th and April 15th 2020 (there are gaps)
- Import Twitter JSON data into ORA-PRO
  - ORA-PRO handles creating derived networks and basic stats.
- Reporting and network visualizations

Source:
IDeaS Center, CMU

Hashtag Collection

Category	Hashtags			
General	#insiderthreat	#insiderattack	#cyberespionage	#dataloss
Corporate	#industrialespionage	#tradesecrets	#embezzlement	#embezzling
Nation-state	#militarysecrets	#spy	#spying	#spies

Source:
IDeaS Center, CMU

Data Description

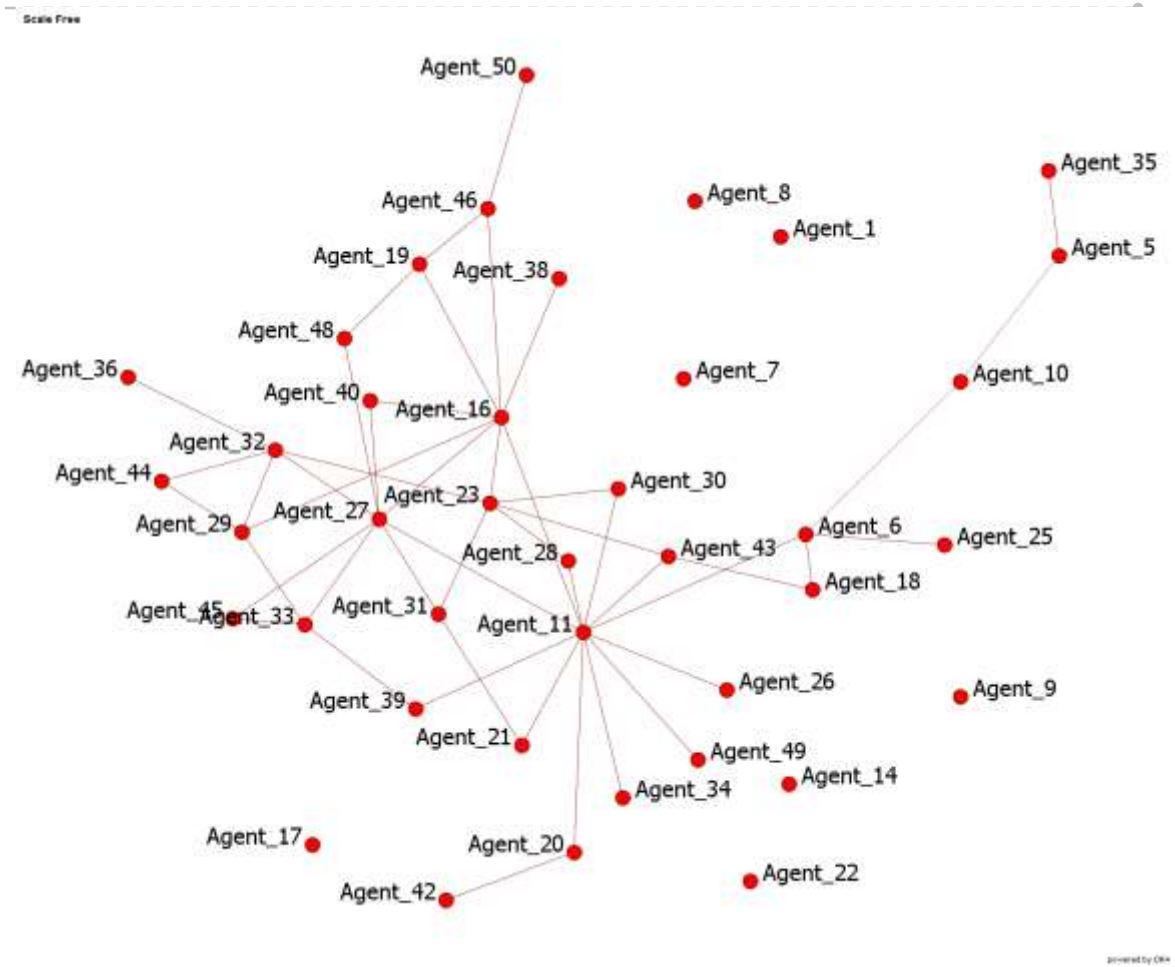
Network	Twitter JSON All Hashtags
First tweet date	2013-01-15 07:06:07-05
Last tweet date	2020-04-15 08:45:03-04
Number of tweets	13640
Number of tweets with geotag	9
Number of tweets with URL	4939
Number of retweets	5826
Number of tweeters	6260
Number of verified tweeters	145
Number of news agency tweeters	17
Number of mentions	4233
Number of distinct hashtags	6795
Number of distinct hashtags used more than once	3212
Number of distinct words	0
Number of distinct words used more than once	0
Number of distinct locations	9

Source: IDeaS Center, CMU

Understanding Networks

- Node – red circles
- Links (Edges) – lines between nodes
- Unidirectional or bidirectional (asymmetric)

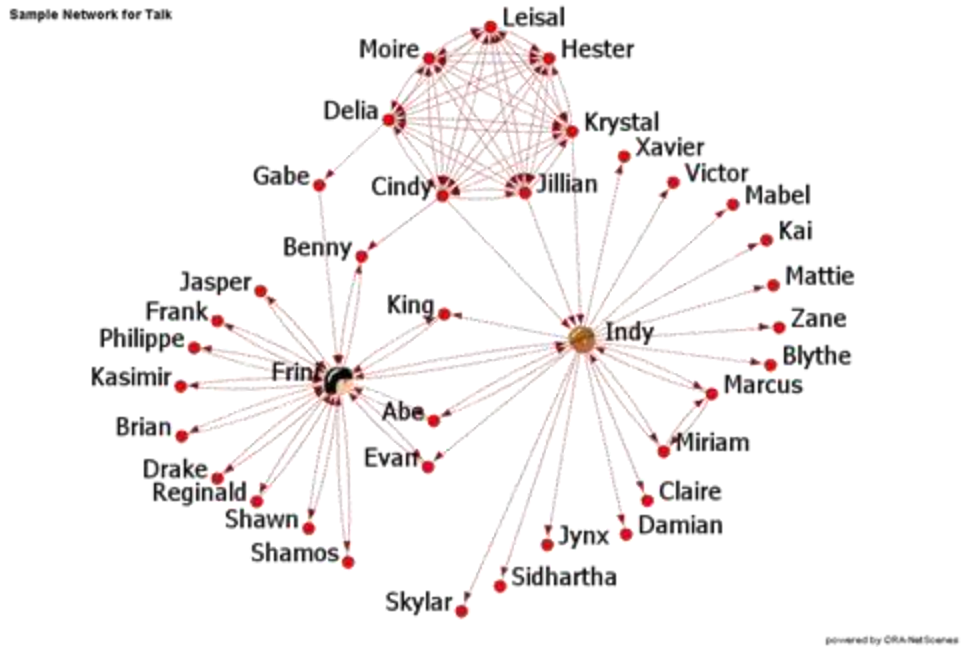
- Can be multi-modal (different types of nodes)
- Or multi-plex (different types of links)



Source: IDeaS Center, CMU

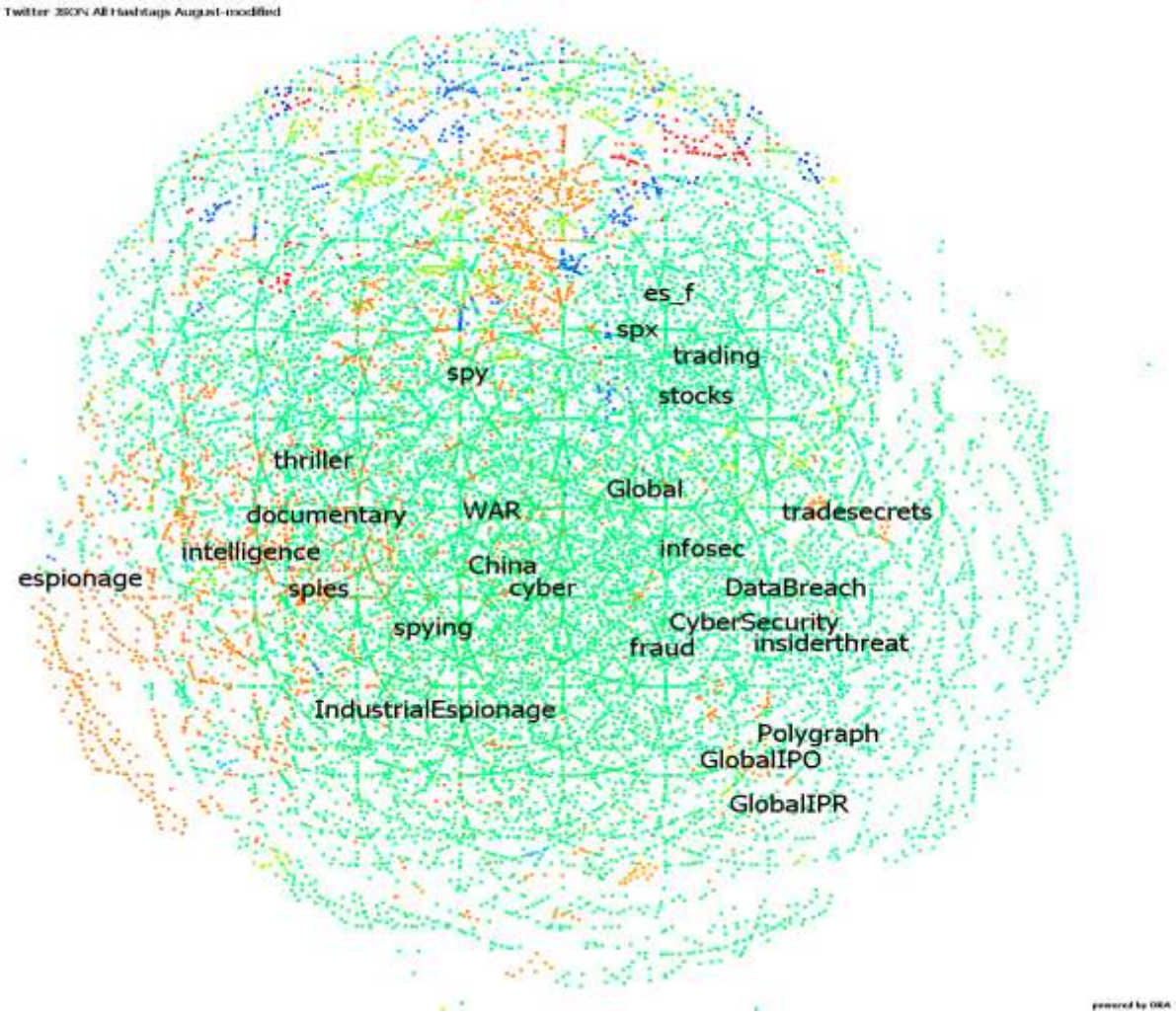
Key Network Terms – Finding Actors of Interest

- Super-spreader
  - A communicator who has **exceptional ability to spread** information
- Super-friends
  - A communicator who is exceptionally involved in dialogue with others (**reciprocal communication**)
- Echo Chamber
  - A group of users and topics that are **strongly interconnected** at both the social and the knowledge level



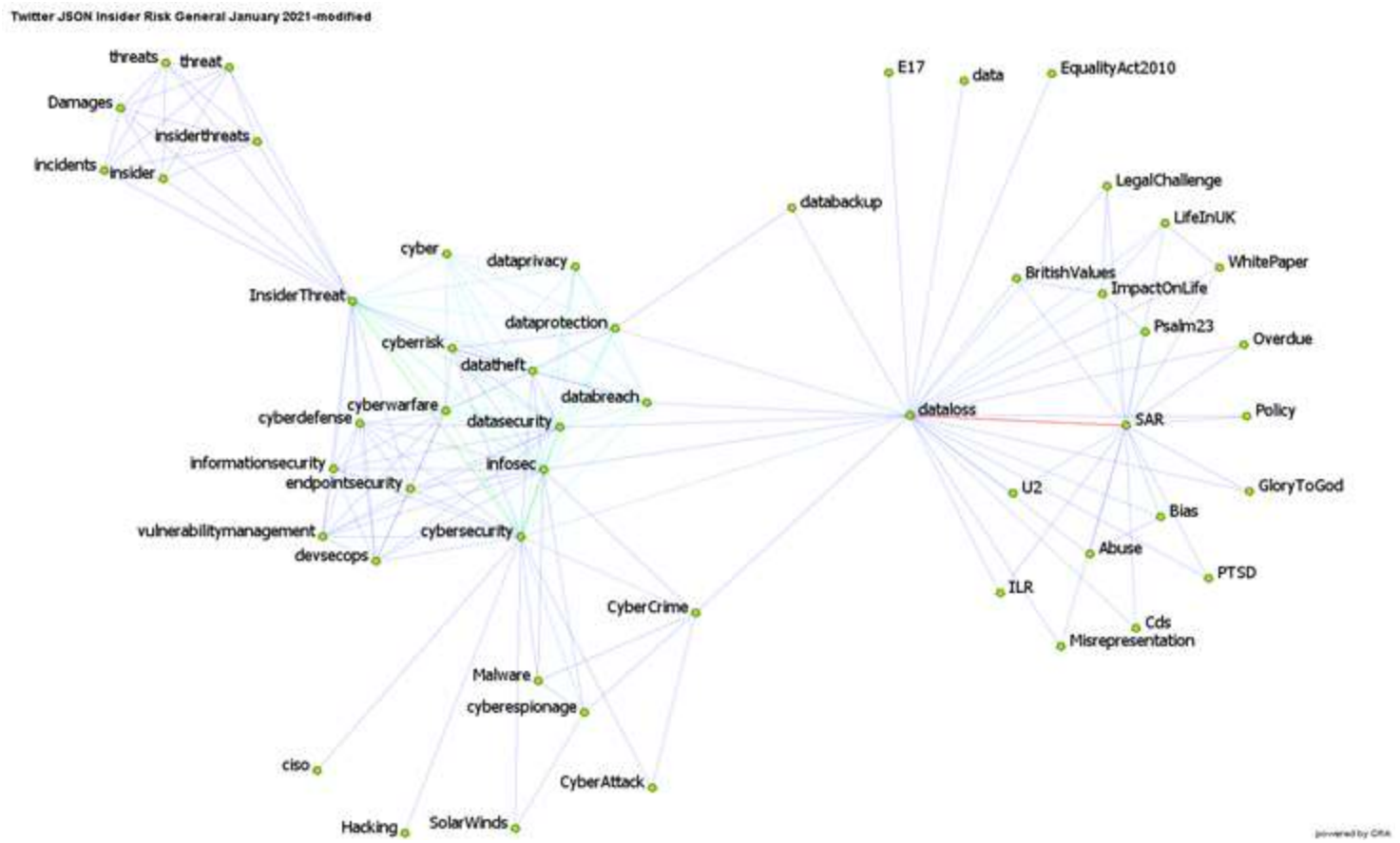
Source: IDeaS Center, CMU

Top Hashtag Visualization

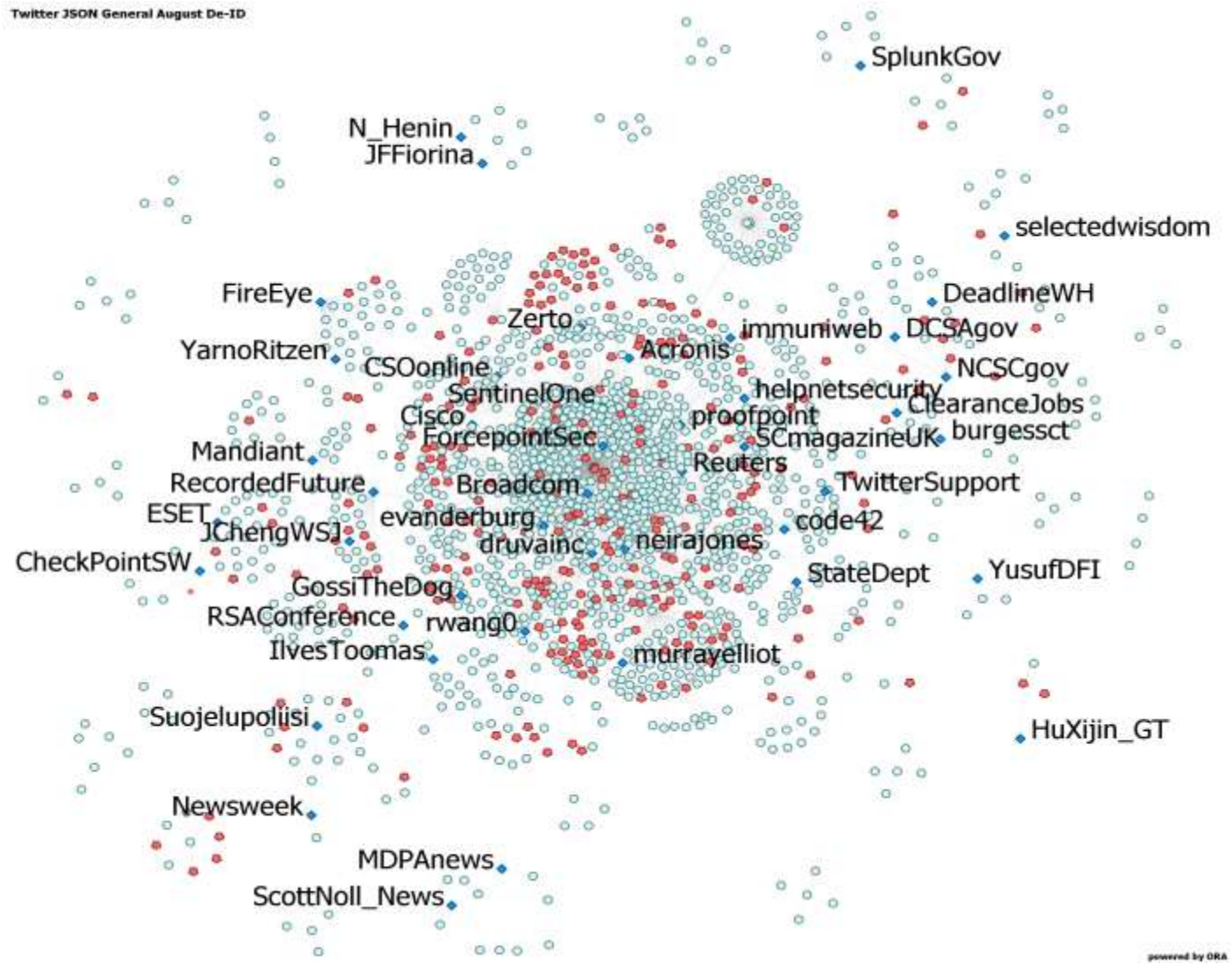


Source: IDeaS Center, CMU

Hashtag Co-occurrence Network (General grouping)



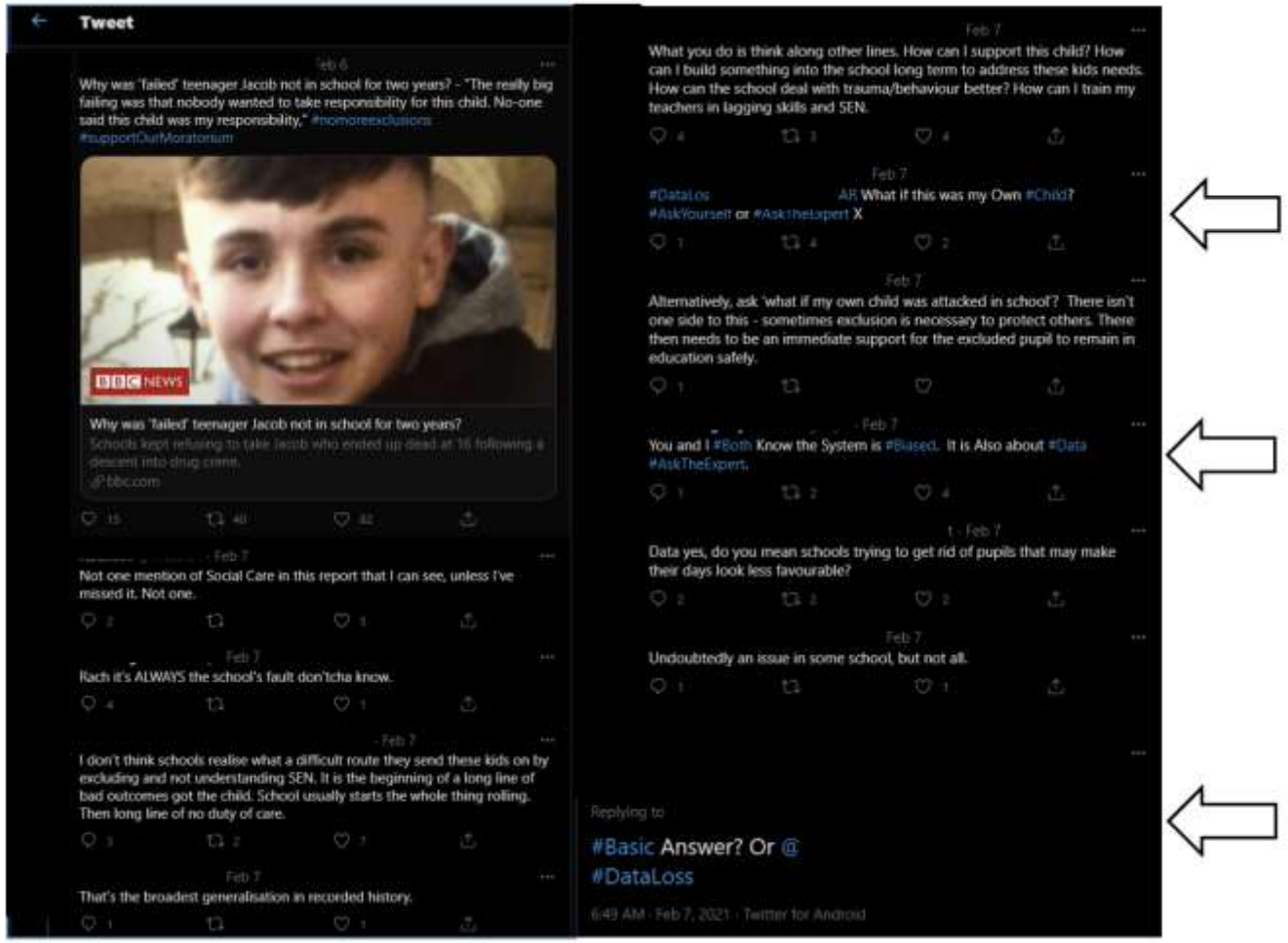
Source:
IDeaS Center, CMU



Standard Users
Verified Users
Bots

Source:
IDeaS Center, CMU

Conversations with Bots

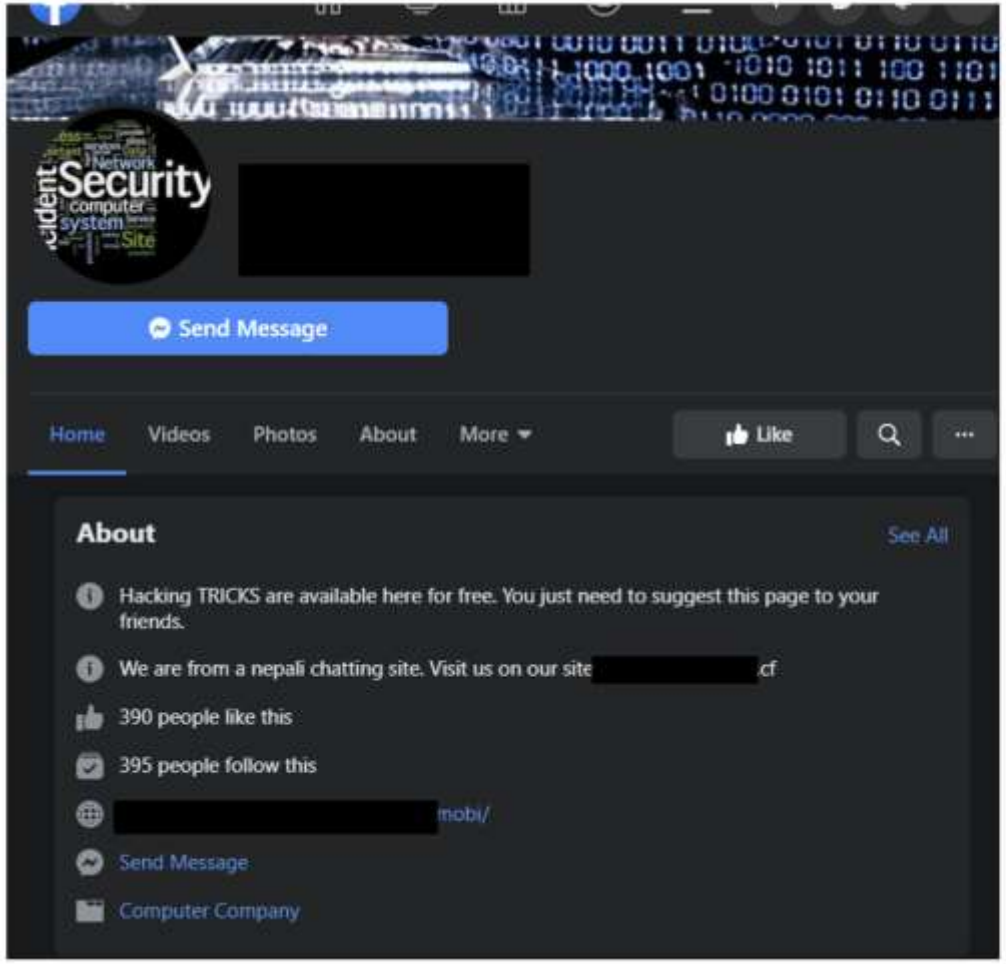


Source:
IDeaS Center, CMU

Bogus Security Accounts – Legitimate followers

Source:
IDeaS Center, CMU

Presence on Other Platforms



Source: IDeaS Center, CMU

Findings and Takeaways

- Autonomous agents (bots) or semi autonomous agents (cyborgs) are present in public forum discussion

- Studying the public conversation around a topic enables us to gain cyber situational awareness – Studying Insider Risk on Twitter is just one example

  Characterizing Public Conversations -> Social Cybersecurity

- Understanding the public conversation can help us understand how to maintain and bolster organizational resilience

Source:
IDeaS Center, CMU

What can we do?

Inoculation against MDM -> Increase Organizational resilience

- The importance of positive deterrence
  - From Big Brother to Good Employer
  - Analogous to “hardening the workforce”
- MDM Awareness
  - Think before you share
  - Fact checking
  - Media Literacy

Future work

- Can we identify when insiders become susceptible?
  - Draw on social sciences:
    - Reactance
    - Normative conflict
    - Social identity theory
    - Social influence theory
- Can we identify ways to recruit insider via information campaigns?
- Computational Modeling
    - Inform models with network data
    - Can we simulate base rates of insider influence
        - … and then, simulate policy interventions?
    - **Inside** - **outside**

Mr. **Luke Osterritter**
Cybersecurity Researcher
CERT Division, Software Engineering Institute, Carnegie Mellon
CASOS/IDeaS, Institute for Software Research, Carnegie Mellon

losterritter@sei.cmu.edu
https://www.sei.cmu.edu/our-work/insider-threat/
https://www.cmu.edu/ideas-social-cybersecurity/

C-InT SBS 2022 summit

C-InT SBS 2022 summit

Thank You

the ThreatLab
Integrating Research Into Practice