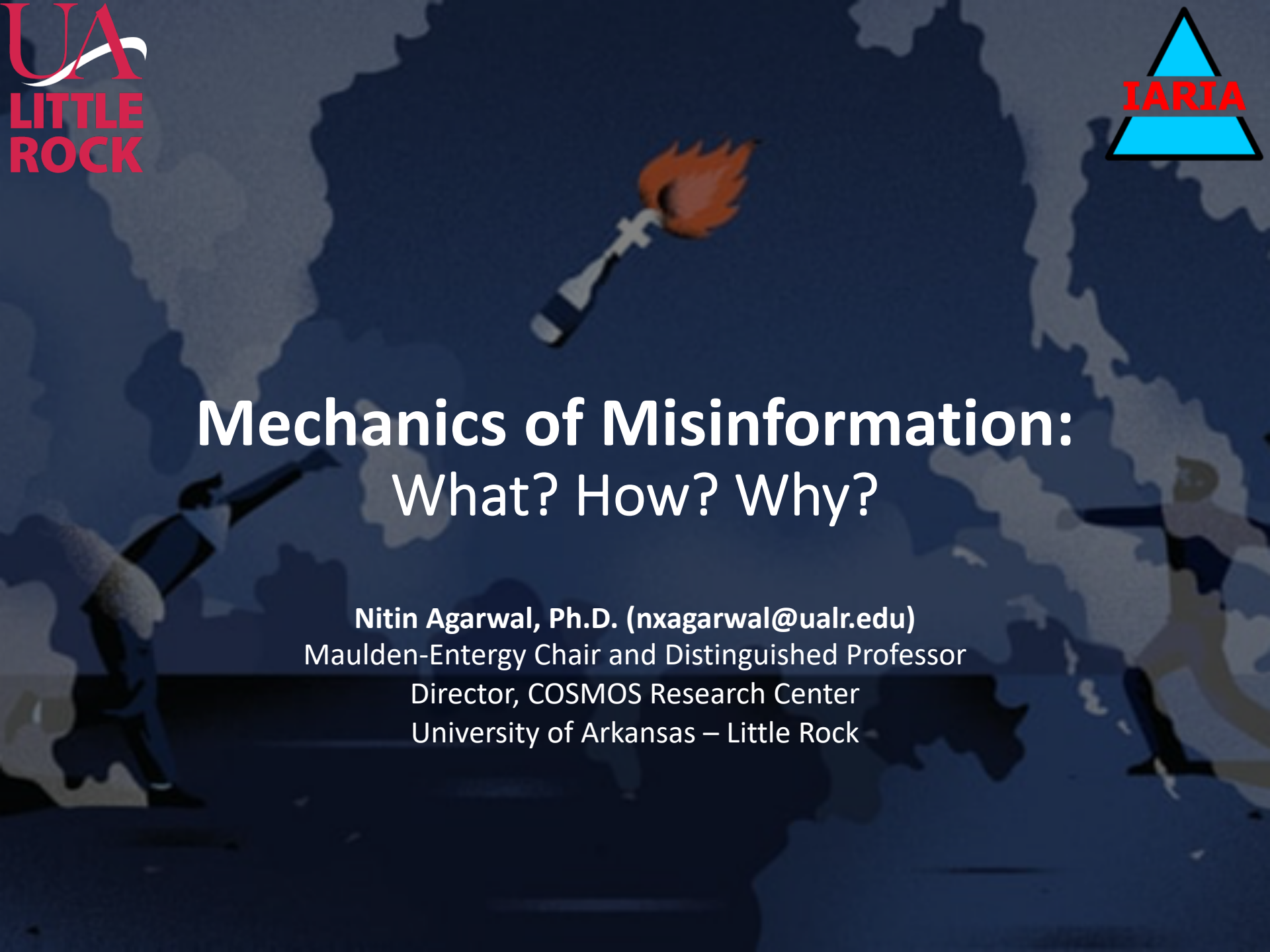


Mechanics of Misinformation:
What? How? Why?

Nitin Agarwal, Ph.D. (nxagarwal@ualr.edu)
Maulden-Entergy Chair and Distinguished Professor
Director, COSMOS Research Center
University of Arkansas – Little Rock

Presenter Bio

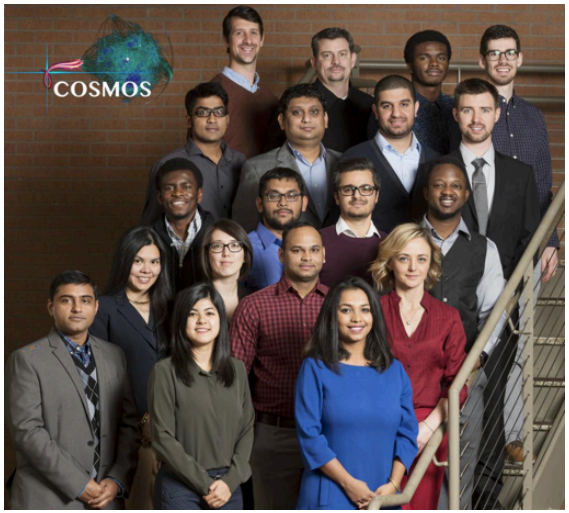
- Director, Collaboratorium for Social Media and Online Behavioral Studies (COSMOS)
- Jerry L. Maulden-Entergy Endowed Chair & Distinguished Professor of Information Science, University of Arkansas – Little Rock
- Research expertise: cyber social behaviors, mis/disinformation analysis, smart health, AI, social computing
- Leading projects with a combined funding of over $20 million from U.S. federal agencies including Department of Defense, DARPA, Department of State, National Science Foundation, Department of Homeland Security.
- Published 10 books and over 200 with several best paper awards and nominations.
- Developed publicly available social media analysis tools (bTracker and vTracker), assisting NATO, European Defense agencies, Australian DoD, Singapore government, Arkansas Attorney General's office, among others. Technologies are listed under National Tech Innovation Hub launched by the U.S. Department of State to defeat foreign based propaganda.
- Covered by local, national, and international media including Bloomberg, US News, KUAR, Arkansas Business, Arkansas Times, Arkansas Democrat Gazette, and many others.
- Spoke at over 100 public and professional, national and international forums such as the NATO, DARPA, US Department of State, US Department of Defense, US Pentagon, US National Academies of Sciences Engineering and Medicine, US Office of the Director of National Intelligence, Facebook Asia Pacific HQ, Twitter Asia Pacific HQ, US Embassy in Singapore, Singapore Ministry of Communication and Information, USIP, among others.
- Fellow of IARIA, AAoC, ARA
- Received University-wide Faculty Excellence Award in Research and Creative Endeavors in 2015 and 2021, Visionary Arkansan, Top 20 in their 20ies, best social media educator, and several other awards.

Dr. Nitin Agarwal
http://cosmos.ualr.edu/
nxagarwal@ualr.edu

COSMOS

Collaboratorium for Social Media and Online Behavioral Studies

COSMOS is developing big data analytical tools to understand digital behaviors and forecast trends to achieve social good. With multi-year multi-million dollar funding from various federal and state agencies, COSMOS is able to bring together several international academic, industry, and government institutions as partners in this venture.



@cosmographers

https://cosmos.ualr.edu/

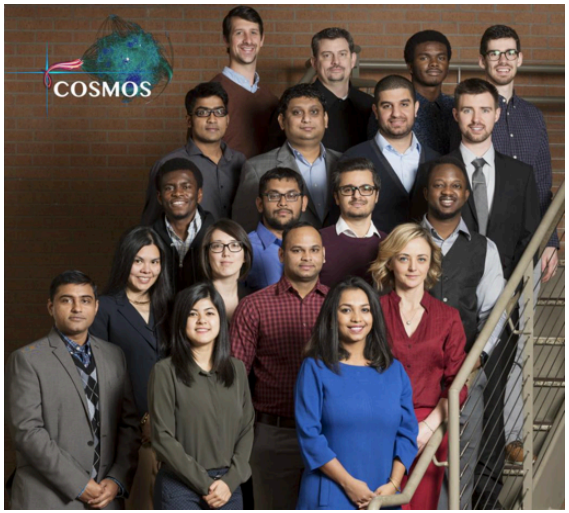
Research Projects

26 grants (total funding over $45 million and $10 million to COSMOS-UALR):

- Army Research Office
- Office of Naval Research
- Air Force Research Lab
- DARPA
- Department of State
- Department of Homeland Security
- National Science Foundation
- NATO
- Arkansas Research Alliance
- Jerry L. Maulden/Entergy Endowment

Cosmographers

- Over 30 members
  - Undergraduate students,
  - Graduate students (MS, PHD)
  - Postdoctoral fellows
  - Administrative staff
- Over 20 graduated
  - Industry (Walmart, Acxiom, FirstOrion, Windstream, Dillard, Amazon, LinkedIn, HP, Cisco)
  - Academia
  - Pursuing higher education



@cosmographers

https://cosmos.ualr.edu/

Collaborators

Academics

- Arizona State University, Carnegie Mellon University, Creighton University, Emory University, University of Central Oklahoma, University of North Carolina-Chapel Hill, George Mason University, George Washington University, University of Pittsburgh, Penn State, University of Memphis, University of New Haven, University of Hawaii, University of Michigan, University of Southern California, West Virginia University, Vilnius University, National University of Singapore, University of Sydney

Industry

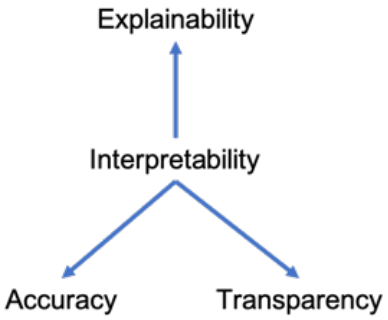
- Atlantic Council (DFRLab), Wal-Mart Inc., LinkedIn, Intelligent Automation Inc., Charles River Analytics, Galisteo Consulting Inc., CarleyTech, Netanomics, Kairos Inc., Bond.AI (fintech)

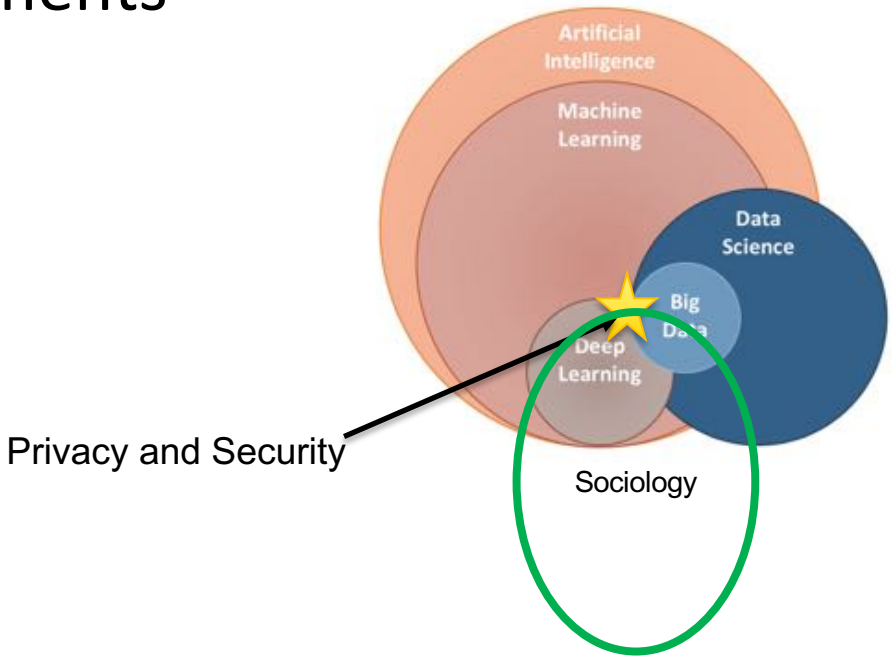
Government

- AR Attorney General's Office, US Defense Agencies, US ARCENT, EUCOM, US Cyber Command, Naval Postgraduate School, US SPAWAR, US Joint Information Operations Warfare Center, III-Marine Expeditionary Force (III-MEF), Army Research Lab, Office of Naval Research (Global), Air Force Research Lab, Singapore Government, Canadian PMO, NATO, StratCom COE, European Defense Agencies, FVEYS – intelligence coalition

Research Thrusts

- Smart Health and AI
- Campaigns and Movements
- Deviant Behaviors
- Social Cybersecurity



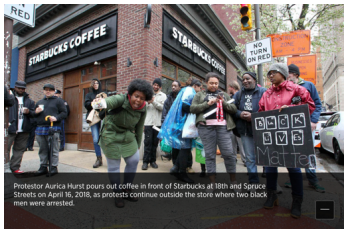


Campaigns and Movements

Flash Mobs in Public Places

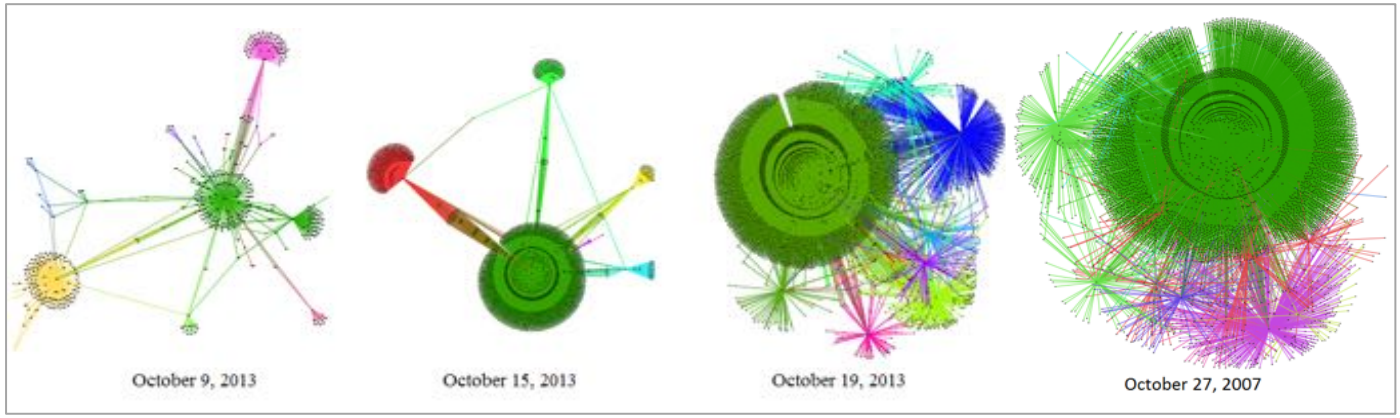
Saudi Women's Right to Drive protest

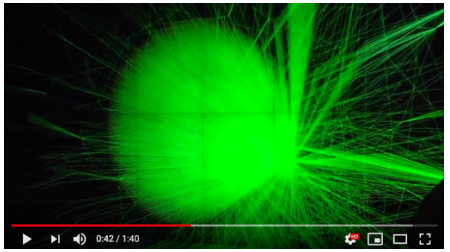
Autism Awareness Campaign



Starbucks Racial Controversy

2011 Arab Spring Social Movement





NSF and DoD funded projects (over $1,000,000) on advancing understanding of cyber-collective actions

Deviant Behaviors

Weaponizing Narratives

Deviant Hackers Networks (DHNs)

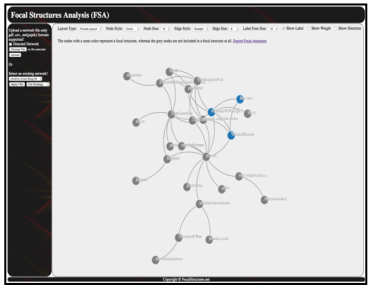
ISIS Recruitment Radicalization Propaganda

Anti NATO Propaganda

Anti-West Narrative

Fake News

Several multi-year DoD funded studies totaling over $10 million



DEPARTMENT OF THE NAVY · ONR · Science & Technology

SCIENCE TO SHAPE THE FUTURE OF THE ARMY · ARMY RESEARCH OFFICE · 1951

U.S. DEPARTMENT OF HOMELAND SECURITY

DEPARTMENT OF STATE · UNITED STATES OF AMERICA

AIR FORCE RESEARCH LABORATORY

DARPA

Ongoing Efforts

- Tracking anti-West, anti-EU, anti-NATO propaganda and influence campaigns
- Participated in various NATO exercises to assist public affairs in social media monitoring

Dragoon Ride 2015

Trident Juncture 2015

Brilliant Jump 2016

Anakonda 2016

Trident Juncture 2018

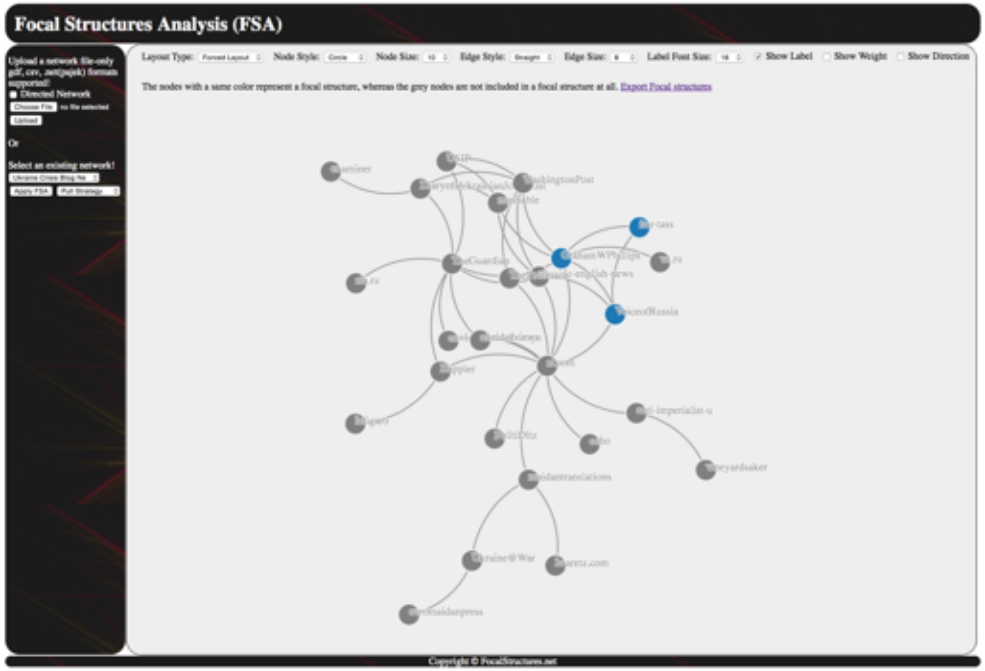
Baltic Operations 2019

- Study terrorist and hacker groups
- Study 2019 Canadian Elections
- Monitor disinformation campaigns in the Asia Pacific region (Singapore Ministry of Communication and Information, Australian DoD, Univ. of Sydney)
- Monitor COVID-19 disinformation campaigns (FVEYS intelligence coalition, Arkansas Attorney General office)

Social Media and Influence Operations

- Key coordinating pro-Russian actors during Ukraine-Russia conflict (Crimean annexation)
- A sample of blog network for Russia-Ukraine conflict containing 18,000 blog posts from 26 blogs.

- **Nodes** represent blogs and **Edges** represent link between blogs (out-links).
- The structure with **blue nodes** is identified as a focal/coordinating structure.
- Although RT.COM is the most central node, the triad "**Graham Phillips – Russian News Agency – Voice of Russia** " is a more influential coordinating structure for information dissemination.



Published in SNAM 2016

Social Media and Influence Operations

- Graham W. Phillips is a British journalist and blogger.
- He went to Ukraine to cover the voice of Ukrainians during Euromaidan.
- He reported that Ukrainians are “happy” with the previous pro-Russian government of Ukraine.
- He used Vlogging to cover the events.
- His Vlogs made him an influential blogger & an enemy to the current Ukrainian government so they banned him from entering Ukraine for three years.
- Once he was banned from entering Ukraine he went to Russia instead of going back to England.

WORLD

How A British Blogger Became An Unlikely Star Of The Ukraine Conflict — And Russia Today

Graham Phillips has become a fixture on Kremlin television and a micro-celebrity on the streets of Ukraine.

Posted on May 20, 2014, at 12:00 p.m.

Max Seddon
BuzzFeed News World Correspondent

More

Graham Phillips has won internet notoriety for his guerrilla field reports from eastern Ukraine for Kremlin TV.
Via Facebook: eurokhariov

Influence Operations and Focal Structures

$$max \sum_{i=1}^{n} \delta_i \quad (1)$$

Subject to

$$\delta_i = \{d\vec{c}_1 \preccurlyeq d\vec{c}_2 \preccurlyeq d\vec{c}_3 \preccurlyeq \cdots \preccurlyeq d\vec{c}_i\} - \overline{dc_j^Q} \quad \forall i,j \quad (2)$$

$$d_i^c = \sum_j m_{ij} \quad \forall i \quad (3)$$

$$d_i^c \geq 2 \quad \forall i \quad (4)$$

$$D_G^L = \frac{1}{n}\sum_{i=1}^{n} d_i^c \quad (5)$$

$$D_G^L < d_i^c \leq D_G^U \quad \forall i \quad (6)$$

$$a_i^c = \frac{(\#\ of\ Triangles) \times 3}{\#\ of\ Connected\ Triples\ of\ Nodes} \quad \forall i \quad (7)$$

$$AC_G^L = \frac{1}{n}\sum_{i=1}^{n} a_i^c \quad (8)$$

$$AC_G^L < a_i^c \leq AC_G^U \quad \forall i \quad (9)$$

$$\overrightarrow{C_v} = \{\overrightarrow{c_1}, \overrightarrow{c_2}, \overrightarrow{c_3}, \dots, \overrightarrow{c_i}\} - \overline{c_j^Q} \quad \forall i,j \quad (10)$$

$$\overline{\vec{c}\delta}_{i_{n\times k}} = \overrightarrow{C_{\delta_i}} \quad \forall i \quad (11)$$

$$F = \left\{c_0, \overline{c_j^Q}, \overline{c_{j+1}^Q}, \dots, \overline{c_\kappa^Q}\right\} \quad \forall j,\kappa \quad (12)$$

$$max \sum_{j=1}^{n} \varrho_j^M \quad (13)$$

Subject to

$$\varrho_j^M = \{\varrho_1, \varrho_2, \varrho_3, \dots, \varrho_j\} \quad \forall j \quad (14)$$

$$\delta_j = \{\overrightarrow{c_1}, \overrightarrow{c_2}, \overrightarrow{c_3}, \dots, \overrightarrow{c_n}\} - \overline{\vec{c}\delta}_{i_{n\times k}} \quad \forall i,j \quad (15)$$

$$B = A_{ij} - \frac{dd^T}{2g} \quad \forall i,j \quad (16)$$

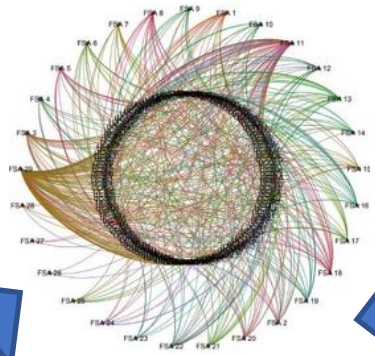
$$\xi_j = \{\overline{\vec{c}\delta}_i \cup \delta_j | \overline{\vec{c}\delta}_i \neq \delta_j\} \quad \forall i,j \quad (17)$$

$$\varrho_j = \frac{1}{2m} Tr\left(\xi_j B \xi_j^T\right) \quad \forall j \quad (18)$$

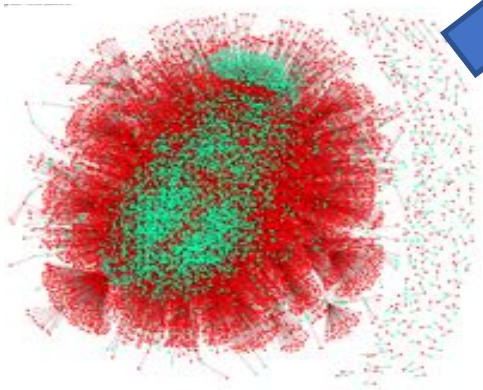
$$\varrho_\square^L \leq \varrho_j \leq \varrho_\square^U \quad \forall j \quad (19)$$

$$c_j^Q = \max\{\varrho_1, \varrho_2, \dots, \varrho_j\} \quad \forall j \quad (20)$$

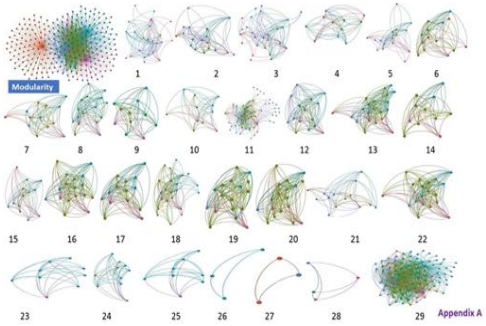
Multi criteria optimization formulation to identify disinformation spreaders. (Alassad, Agarwal, et al., 2021) Central European Journal of Operations Research, Springer



Identifying disinformation spreaders

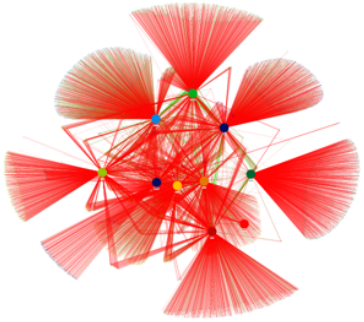


YouTube COVID-19 misinformation video-user network

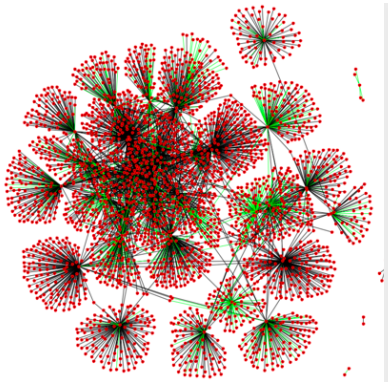


Sorted on effectiveness

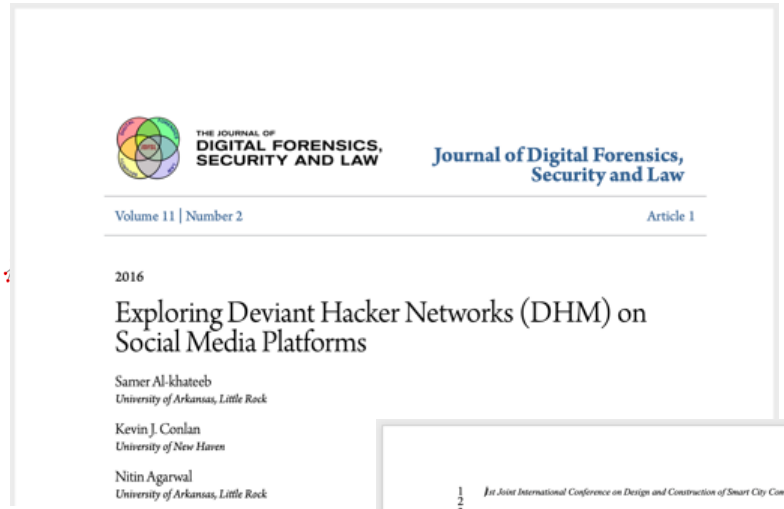
Terrorist and Hacker Networks



ISIS Recruitment Network



Black Hat Hacker Network



THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 11 | Number 2 Article 1

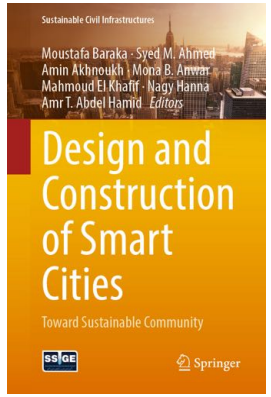
2016

Exploring Deviant Hacker Networks (DHM) on Social Media Platforms

Samer Al-khateeb
University of Arkansas, Little Rock

Kevin J. Conlan
University of New Haven

Nitin Agarwal
University of Arkansas, Little Rock



Sustainable Civil Infrastructures

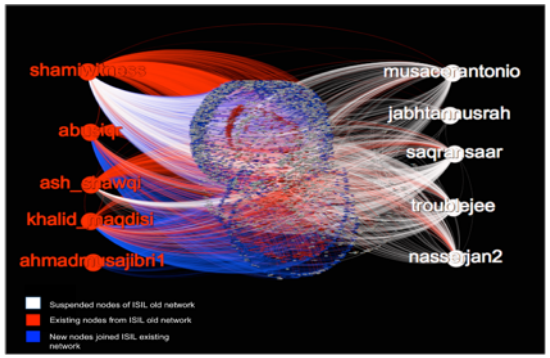
Moustafa Baraka · Syed M. Ahmed
Amin Akhnoukh · Mona B. Anwar
Mahmoud El Khafif · Nagy Hanna
Amr T. Abdel Hamid *Editors*

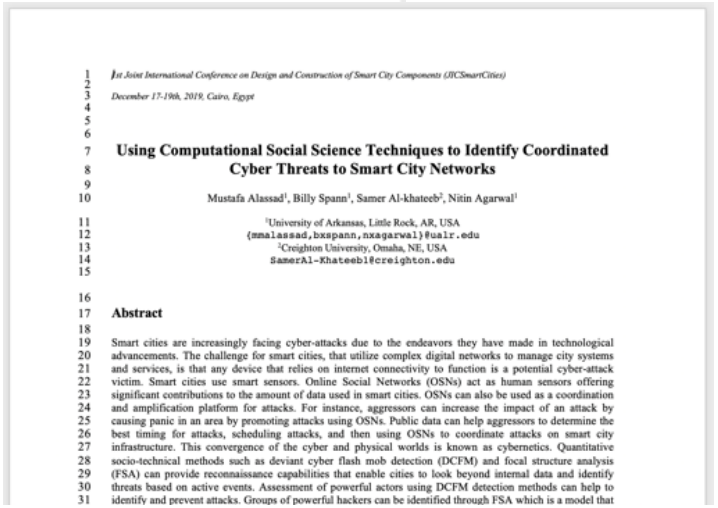
Design and Construction of Smart Cities

Toward Sustainable Community

SSGE

Springer





1st Joint International Conference on Design and Construction of Smart City Components (JICSmartCities)

December 17-19th, 2019, Cairo, Egypt

Using Computational Social Science Techniques to Identify Coordinated Cyber Threats to Smart City Networks

Mustafa Alassad[1], Billy Spann[1], Samer Al-khateeb[2], Nitin Agarwal[1]

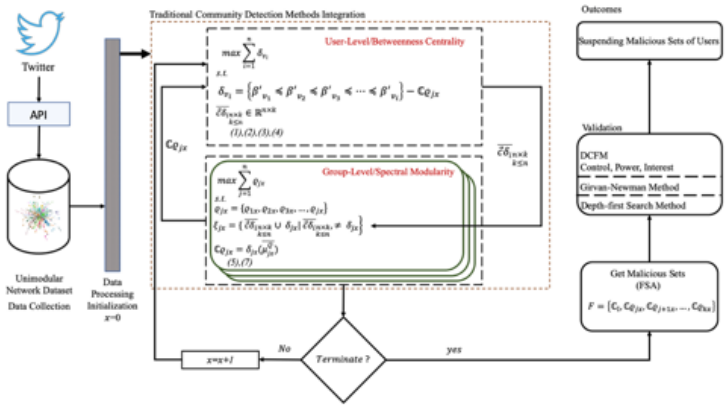
[1]University of Arkansas, Little Rock, AR, USA
{mmalassad,bxspann,nxagarwal}@ualr.edu
[2]Creighton University, Omaha, NE, USA
SamerAl-Khateeb1@creighton.edu

Abstract

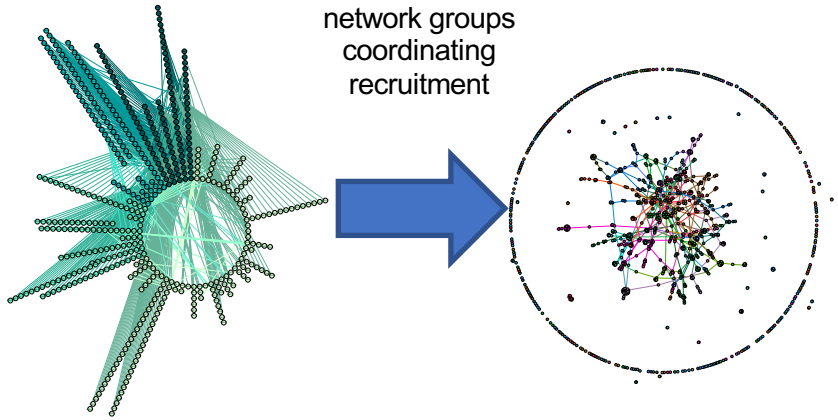
Smart cities are increasingly facing cyber-attacks due to the endeavors they have made in technological advancements. The challenge for smart cities, that utilize complex digital networks to manage city systems and services, is that any device that relies on internet connectivity to function is a potential cyber-attack victim. Smart cities use smart sensors. Online Social Networks (OSNs) act as human sensors offering significant contributions to the amount of data used in smart cities. OSNs can also be used as a coordination and amplification platform for attacks. For instance, aggressors can increase the impact of an attack by causing panic in an area by promoting attacks using OSNs. Public data can help aggressors to determine the best timing for attacks, scheduling attacks, and then using OSNs to coordinate attacks on smart city infrastructure. This convergence of the cyber and physical worlds is known as cybernetics. Quantitative socio-technical methods such as deviant cyber flash mob detection (DCFM) and focal structure analysis (FSA) can provide reconnaissance capabilities that enable cities to look beyond internal data and identify threats based on active events. Assessment of powerful actors using DCFM detection methods can help to identify and prevent attacks. Groups of powerful hackers can be identified through FSA which is a model that

Terrorist and Hacker Networks

Terrorist Networks and Focal Structures



Algebraic transformation of the model to identify key network groups coordinating deviant acts grounded in **Collective Action theory**. (Alassad, Agarwal et al., 2020) Journal of Information Processing and Management, Elsevier

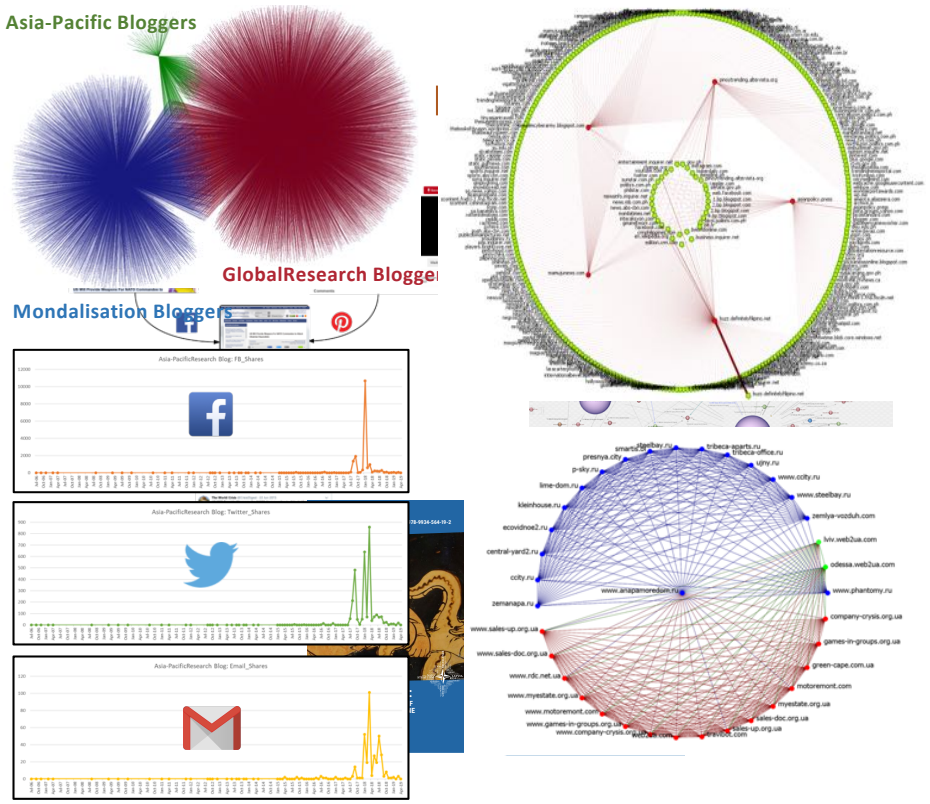


Before
ISIS recruitment network (hub and spoke)

After
ISIS recruitment network disintegrates

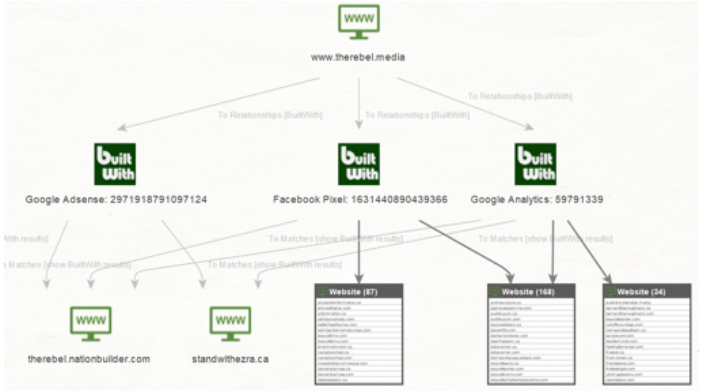
Computational Propaganda Tactics

- Cross platform orchestration
  - Growing use of niche platforms
- Communities and coordination
  - Flash mob style coordination
  - Blogger communities
  - Coordinated clickbait (a.k.a. blog farms, information laundering)
  - Computational (AI) propaganda – coordinated *deepfakes*
- Algorithmic manipulation
  - Machine driven communications (MADCOMs) (bots, botnets, social bots, etc.)



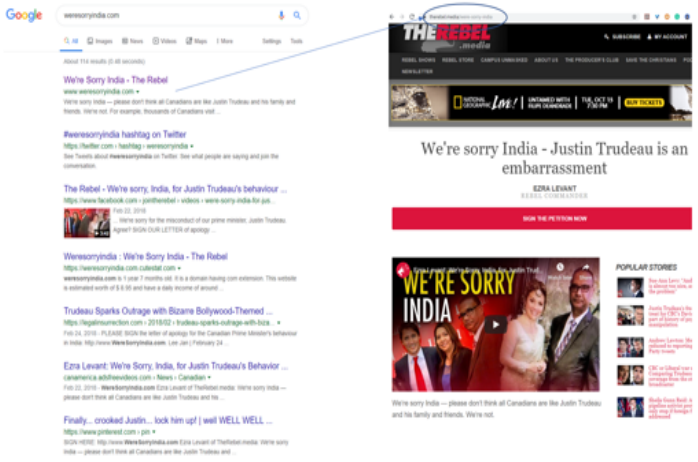
Algorithmic Manipulation

Canadian Federal Elections 2019



Coordinated *deepfakes*

One such fake website "weresorryindia.com" amplified anti-Trudeau narrative suggesting he is not a friend of the Canadian-Indian community. The website tops the results in search engines.



The Canadian Special Operations Forces Command (CANSOFCOM)

Algorithmic Manipulation – TRJE 2018

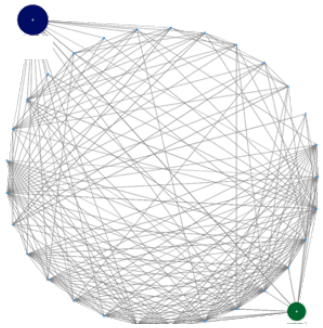
- Environmental Impact
- Disturbs Local Economy
- Mistreatment by NATO Troops
- Mocking/ridiculing NATO
- NATO is a joke – Not a real threat
- 'Stop NATO' Protests/Astroturfing
- Threatening Stability
- NATO poking 'Russian Bear'
- NATO is aggressive

**published in NATO SPS 2019*

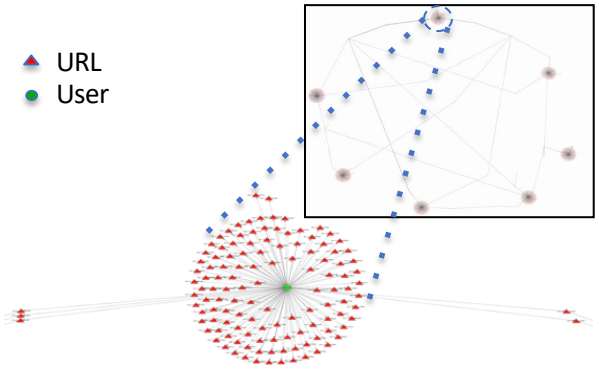
Evolution of Botnets

From bots → botnets → social bots

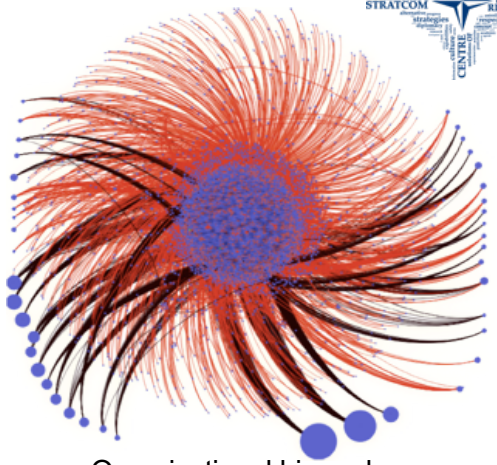
Published by NATO StratCom COE



Mutual reciprocity.
IFYFM & FMIFY



No mutual reciprocity.
Coordination in information network



Organizational hierarchy.
Core and peripheral bots

COORDINATION/BEHAVIOR COMPLEXITY

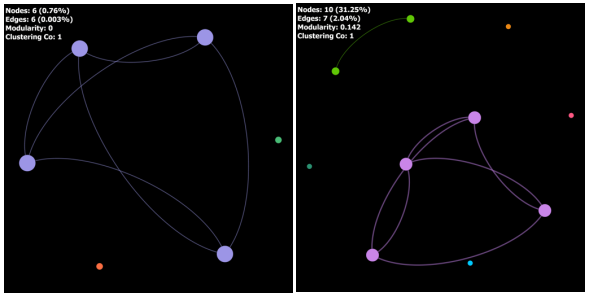
Crimean Invasion 2014

Dragoon Ride 2015

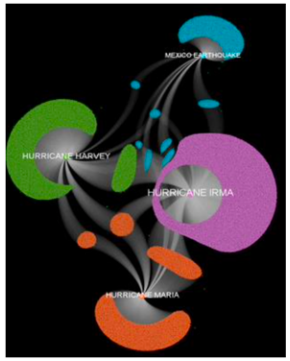
Trident Juncture 2015

ISIS Propaganda 2016

Assessing Botnet Coordination



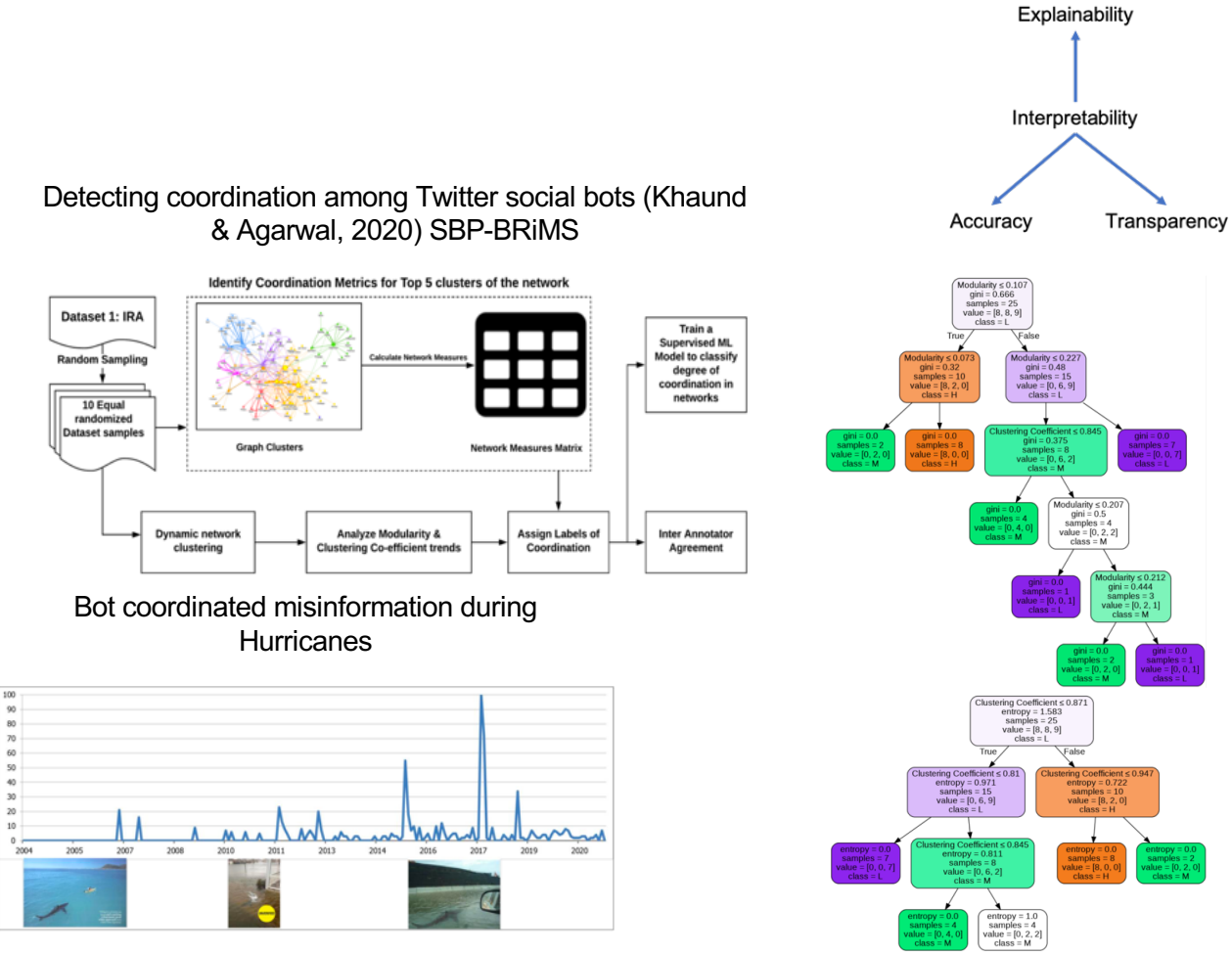
IRA Twitter bot data released by US Intelligence Agencies



Language	Hashtag (Translation)
English	#DACA, #BlackLivesMatter
Spanish	#VenezuelaDemocraciaYDiálogo (Venezuela Democracy and Dialogue), #Cáncer (Cancer)
Arabic	#اسرائيل, (The demise Of Israel) #اليهود (The Jews)
French	#Nucléaire (Nuclear), #GendarmerieEnOpération (Gendarmerie Special Operations)
Mandarin	金正恩 (Kim Jong-un), 核试验 (Nuclear Test)

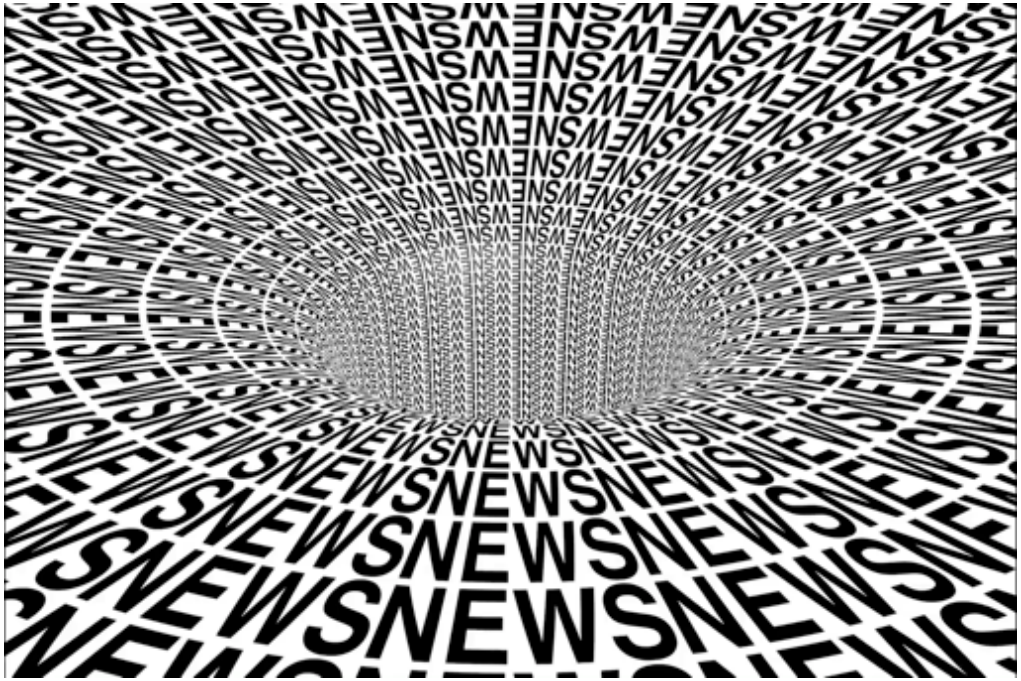
Detecting coordination among Twitter social bots (Khaund & Agarwal, 2020) SBP-BRiMS

Bot coordinated misinformation during Hurricanes



Platform Vulnerability/Bias

- AI-based recommendation algorithms that predict our shopping behaviors, books and articles to read, videos to watch lack transparency.
- Recommendation algorithm learns from behavioral data and perpetuates the underlying bias in its recommendations.
  - YouTube's recommendation algorithm is known to push its viewers down the conspiratorial rabbit hole by suggesting related videos.
  - On Facebook, ads to recruit delivery drivers for Domino's Pizza Inc. were disproportionately shown to men, while women were more likely to receive notices in recruiting shoppers for grocery-delivery service Instacart Inc.
- Explainable model could help in identifying causes of biased recommendations thereby enhancing the model's transparency.



Platform Vulnerability/Bias

Computational propaganda tactics on YouTube detected using a groundbreaking multimedia processing approach based on color theory. Research received Best Paper award at the International Conference on Human and Social Analytics (HUSO), Oct.18-22,2020

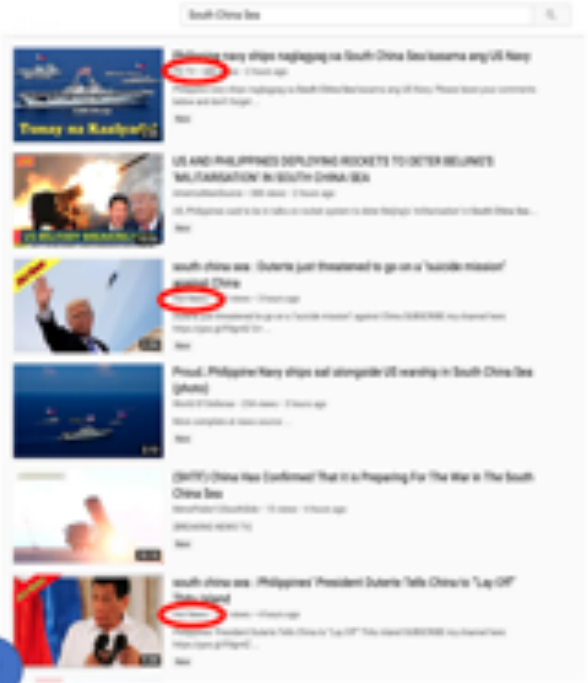
Video ID: OM5vaF2kzPA
Title: China vs US The War in the South China Sea already Start
Channel: Breaking News TV

Video ID: GsCmudyXY2o
Title: China vs US The War in the South China Sea already Start
Channel: DOT COM US

Similar videos detected on different YouTube channels using barcode approach. Below, network of channels identified deploying crowd amplification tactic.

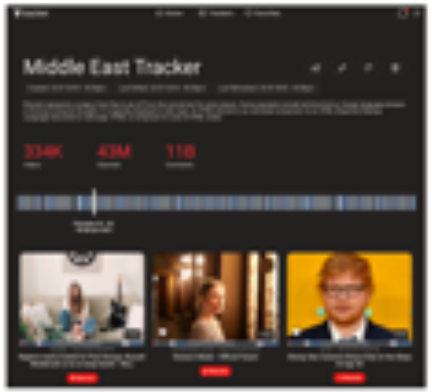
1

Crowd amplification tactic successfully manipulated YouTube's search results. "Hot News" - a prominent channel disseminating anti-US videos related "South China Sea" conflict – shows up at top of the search results.

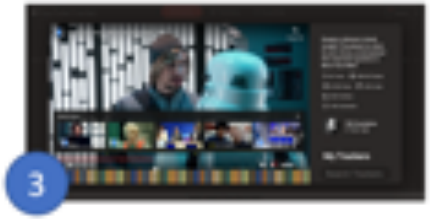


2

Video barcode technique has been transitioned to YouTubeTracker



Video barcode technique allows us to navigate interesting narrative elements for a collection of videos pertaining to an event (above) or a single video (below)



3

Virality over veracity!

Platform Vulnerability/Bias Characterization

How to observe, identify, and measure algorithmic bias?

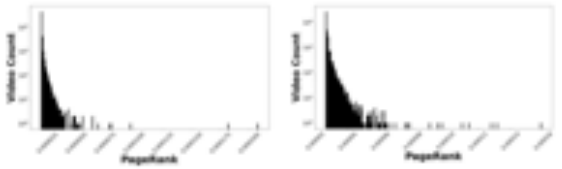


Fig. 1. Distribution of PageRank values in the recommendation graphs 1 (left) and 2 (right). We observe similar results in all recommendation graphs. The count of videos is represented in log scale on the y-axis.

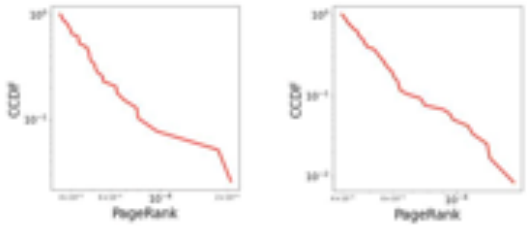
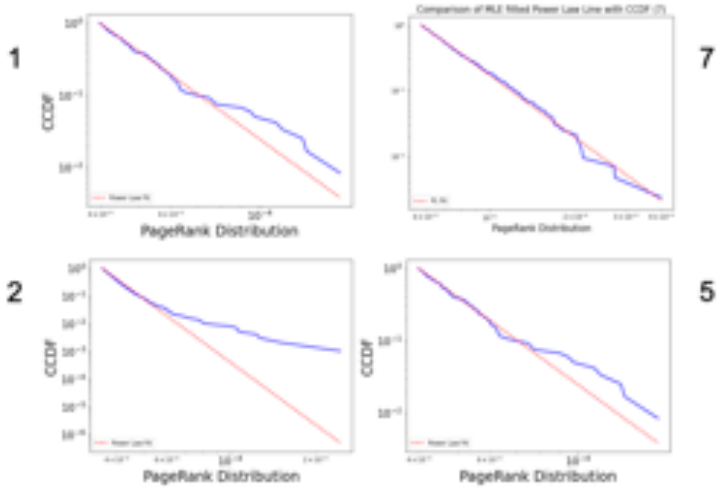


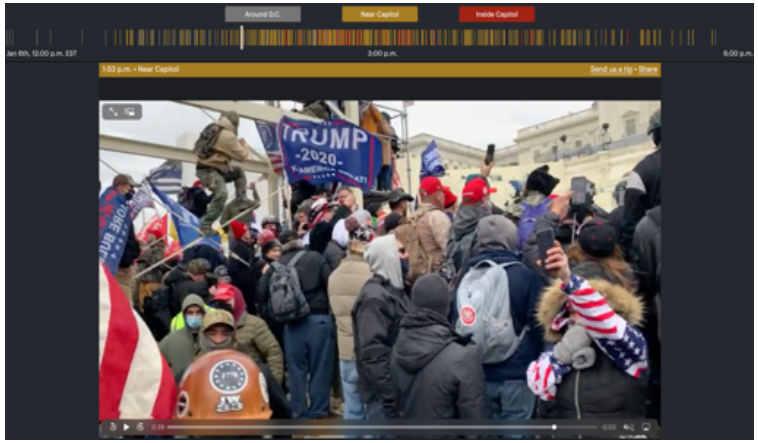
Fig. 2. Complementary Cumulative Distribution Function (CCDF) Plots of PageRank Scores in each Recommendation Graphs 1(left) and 2 (right).

Topic drift and decrease in relevance was observed.

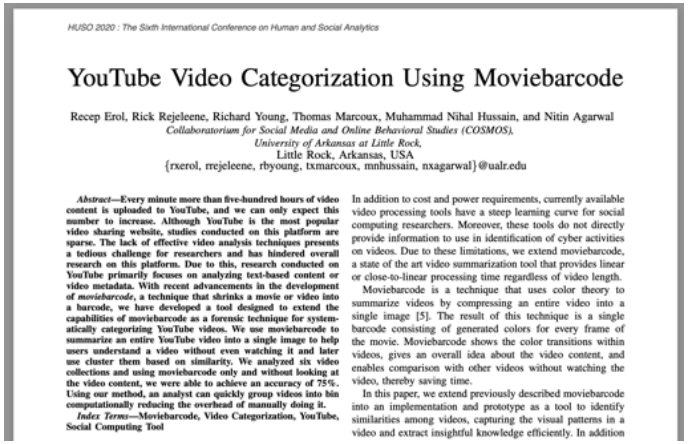


Top PageRank videos were removed weeks or months after their appearance in the recommendation network. Reason for content removal is violation of platform terms and services.

From Cyber to Real-world Mobs



Human and Social Analytics 2020 – Best Paper



HUSO 2020 : The Sixth International Conference on Human and Social Analytics

YouTube Video Categorization Using Moviebarcode

Recep Erol, Rick Rejeleene, Richard Young, Thomas Marcoux, Muhammad Nihal Hussain, and Nitin Agarwal
Collaboratorium for Social Media and Online Behavioral Studies (COSMOS),
University of Arkansas at Little Rock,
Little Rock, Arkansas, USA
{rxerol, rrejeleene, rbyoung, txmarcoux, mnhussain, nxagarwal}@ualr.edu

***Abstract*—Every minute more than five-hundred hours of video content is uploaded to YouTube, and we can only expect this number to increase. Although YouTube is the most popular video sharing website, studies conducted on this platform are sparse. The lack of effective video analysis techniques presents a tedious challenge for researchers and has hindered overall research on this platform. Due to this, research conducted on YouTube primarily focuses on analyzing text-based content or video metadata. With recent advancements in the development of *moviebarcode*, a technique that shrinks a movie or video into a barcode, we have developed a tool designed to extend the capabilities of moviebarcode as a forensic technique for systematically categorizing YouTube videos. We use moviebarcode to summarize an entire YouTube video into a single image to help users understand a video without even watching it and later use cluster them based on similarity. We analyzed six video collections and using moviebarcode only and without looking at the video content, we were able to achieve an accuracy of 75%. Using our method, an analyst can quickly group videos into bin computationally reducing the overhead of manually doing it.**

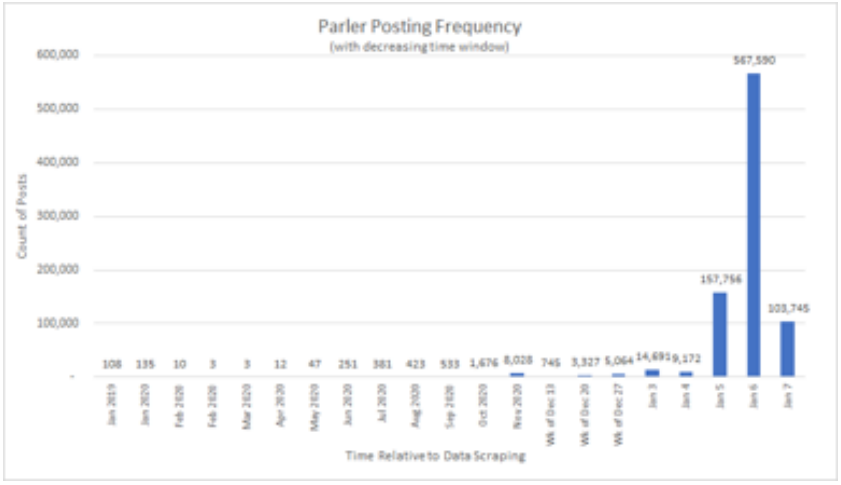
***Index Terms*—Moviebarcode, Video Categorization, YouTube, Social Computing Tool**

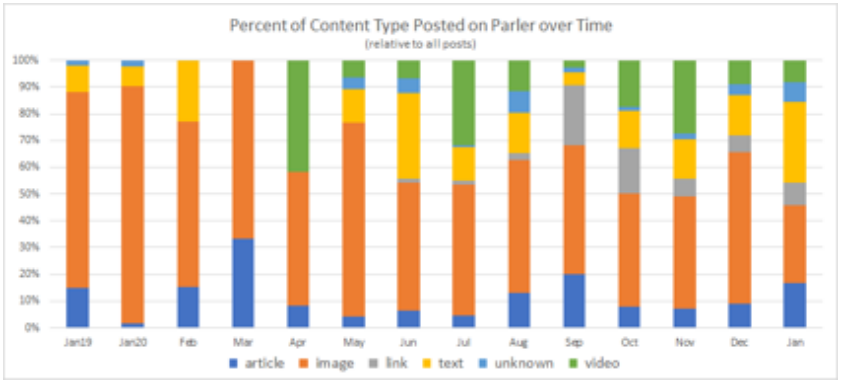
In addition to cost and power requirements, currently available video processing tools have a steep learning curve for social computing researchers. Moreover, these tools do not directly provide information to use in identification of cyber activities on videos. Due to these limitations, we extend moviebarcode, a state of the art video summarization tool that provides linear or close-to-linear processing time regardless of video length.

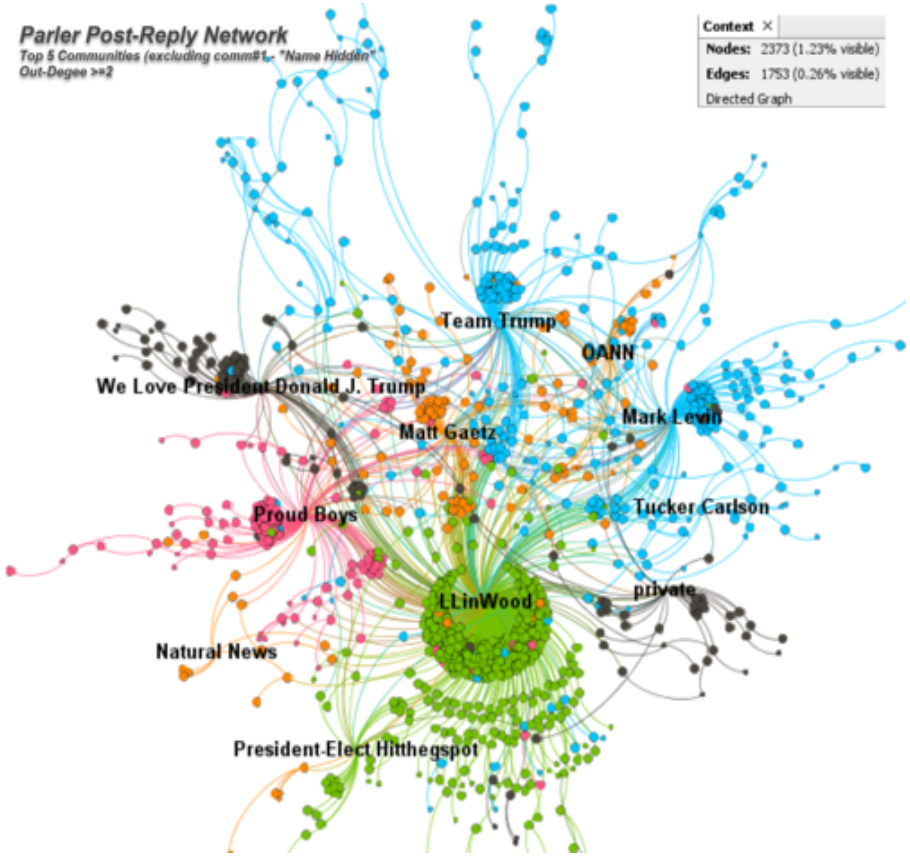
Moviebarcode is a technique that uses color theory to summarize videos by compressing an entire video into a single image [5]. The result of this technique is a single barcode consisting of generated colors for every frame of the movie. Moviebarcode shows the color transitions within videos, gives an overall idea about the video content, and enables comparison with other videos without watching the video, thereby saving time.

In this paper, we extend previously described moviebarcode into an implementation and prototype as a tool to identify similarities among videos, capturing the visual patterns in a video and extract insightful knowledge efficiently. In addition

Mining Parler Data

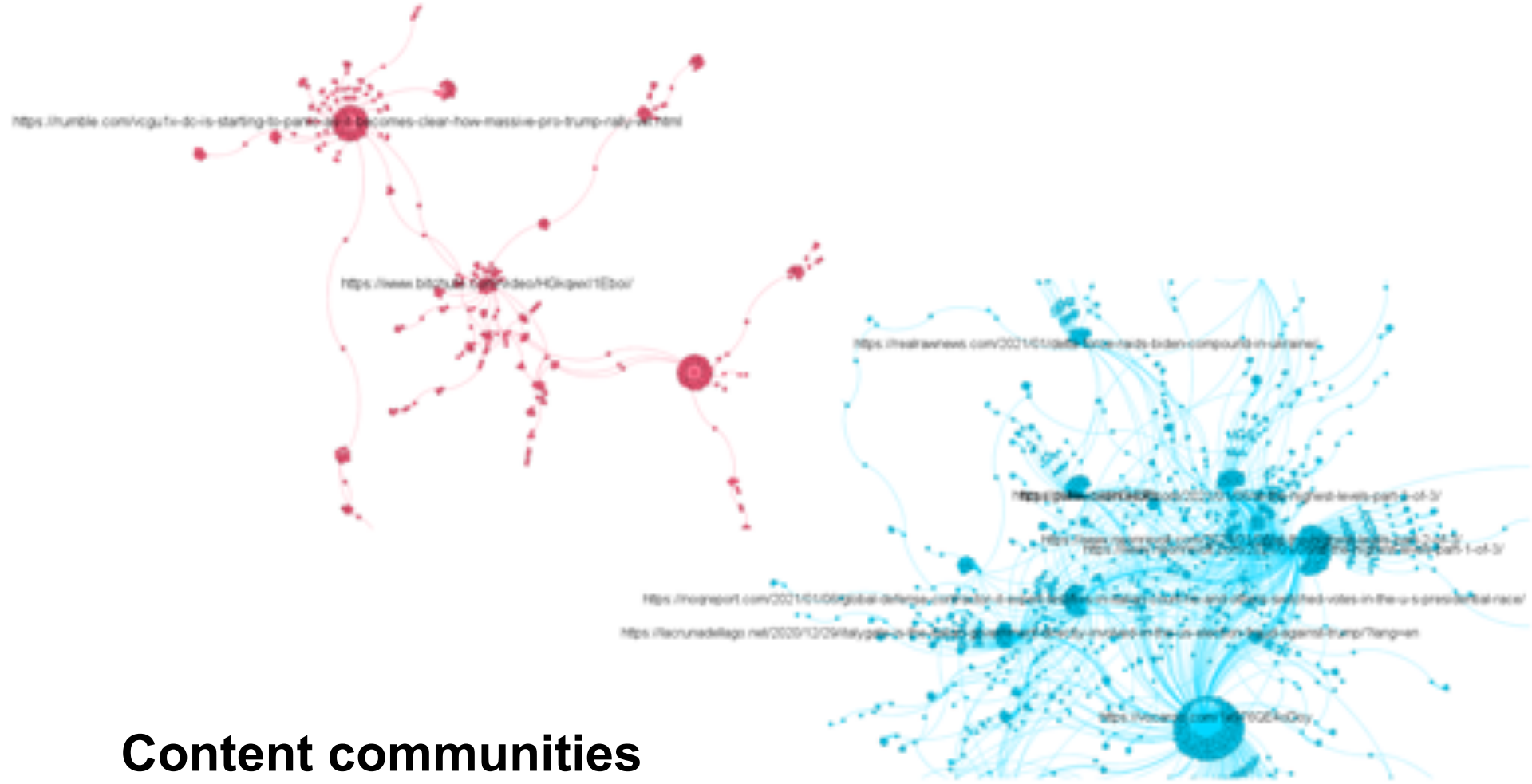






Over 70 Terabytes of data

Mining Parler Data



Content communities

Mining Parler Data

Content communities

Tracking COVID-19 Misinformation

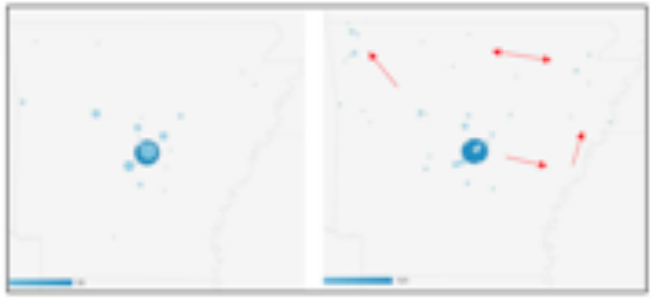
COVID-19 misinfodemic presents an example of emerging cyber-social threats. While there are similarities with other disinformation campaigns (e.g., anti-NATO, anti-US, anti-EU, anti-West in Indo-Pacific region), COVID-19 disinformation campaigns have their nuances such as global and regional narratives; high topical diversity (health, policy, religion, geopolitical affairs, etc.); high volume, velocity, veracity, and variety of false narratives. COVID-19 misinformation tracker tool developed in collaboration with the Arkansas Office of the Attorney General to support detection, investigation, and mitigation of cross-platform COVID-19 disinformation campaigns and scams to assist policy makers. Our efforts demonstrate that when researchers coordinate with policy makers it can make a difference, especially when that coordination remains an ongoing process.

Cross-platform false narratives detected using developed socio-computational methodologies

Education component of the effort

People notify us of scams and other misinformation cases not in our database which are then investigated

Daily reports to the AG's Office with our investigation results and recommendations for enhancing outreach/awareness



May 5, 2020 — Jan 21, 2021

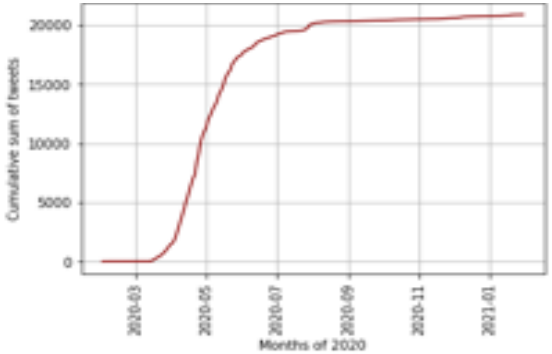
Increased penetration into rural areas of Arkansas as annotated by the arrows in the figure on right demonstrates the effectiveness of the tool and communications strategies.

Arkansas Office of the Attorney General Press Release on our COVID-19 Misinfo Tracker

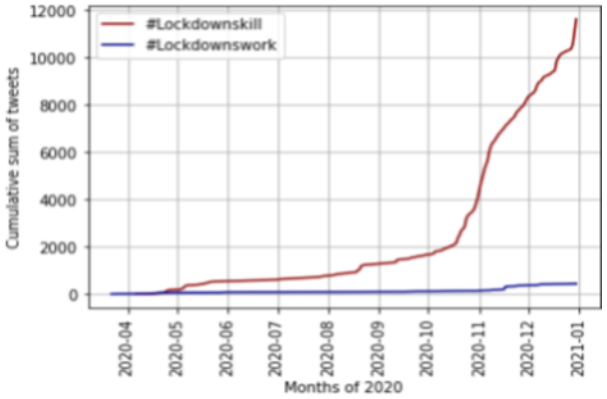
https://cosmos.ualr.edu/covid-19

Tracking COVID-19 Misinformation

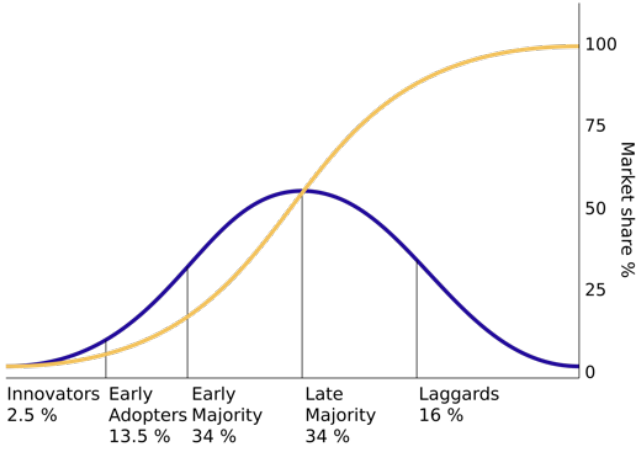
#BillGatesVirus



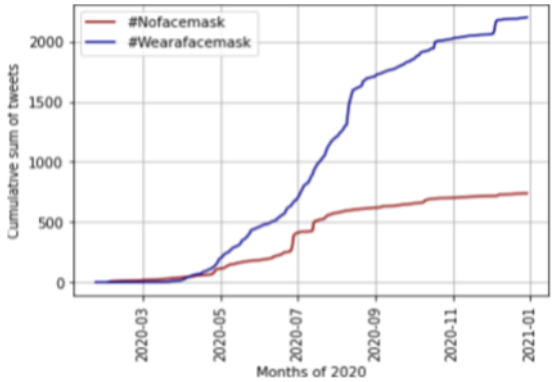
#Lockdownskill vs. #Lockdownswork



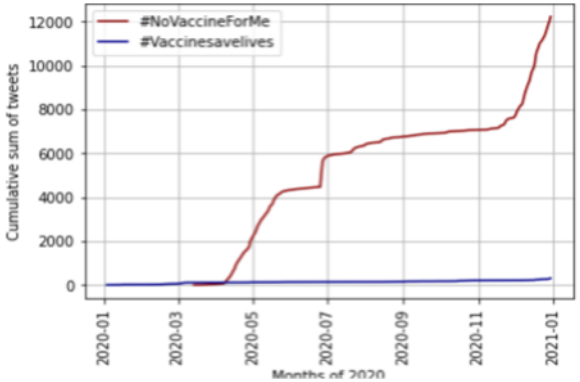
Theory of diffusion of innovations



#Nofacemask vs. #Wearafacemask

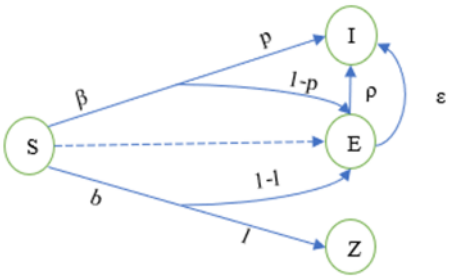


#NoVaccineForMe vs. #Vaccinesaveslives



Modeling Misinfodemic

How misinformation spreads? Leveraging epidemiological model.
(Maleki, Agarwal, et al. 2021) European Conference of Operations Research (EURO) 2021



SEIZ model

- S: Susceptible
- E: Exposed
- I: Infected
- Z: Skeptic

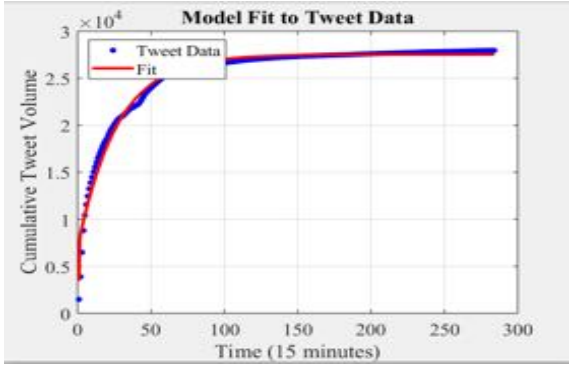
$$\frac{dS}{dt} = -\beta S\frac{I}{N} - bS\frac{Z}{N}$$

$$\frac{dE}{dt} = (1-p)\,\beta S\frac{I}{N} + (1-l)bS\frac{Z}{N} - \rho E\frac{I}{N} - \varepsilon E$$

$$\frac{dI}{dt} = p\beta S\frac{I}{N} + \rho E\frac{I}{N} + \varepsilon E$$

$$\frac{dZ}{dt} = lbS\frac{Z}{N}$$

Parameter	Definition
β	Contact rate between S and I.
b	Contact rate between S and Z.
ρ	Contact rate between E and I.
p	Probability of S to I given contact with I.
1-p	Probability of S to E given contact with I.
ε	Transition rate of E to I (Incubation rate).
l	Probability of S to Z given contact with Z.
1-l	Probability of S to E given contact with Z.

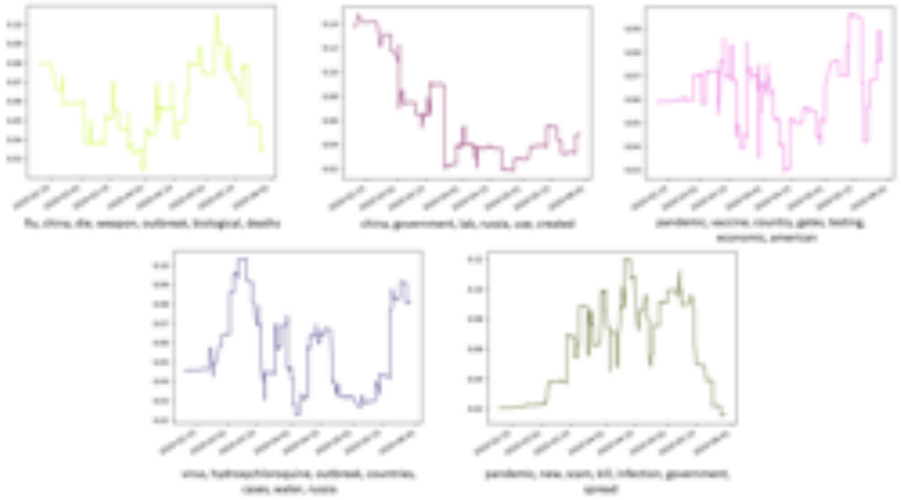


Misinformation regarding the unrest in Washington, D.C. in March 2020 propagated using the #DCblackout hashtag

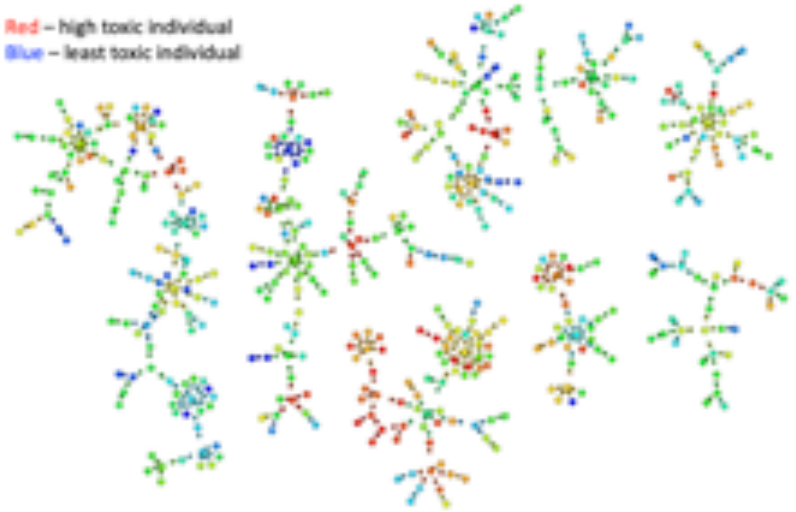
Error = 0.019

Networks and Toxicity

Data collected during the effort led to development of predictive behavioral models to assist policymaking and crisis communications. Two examples are shown below.



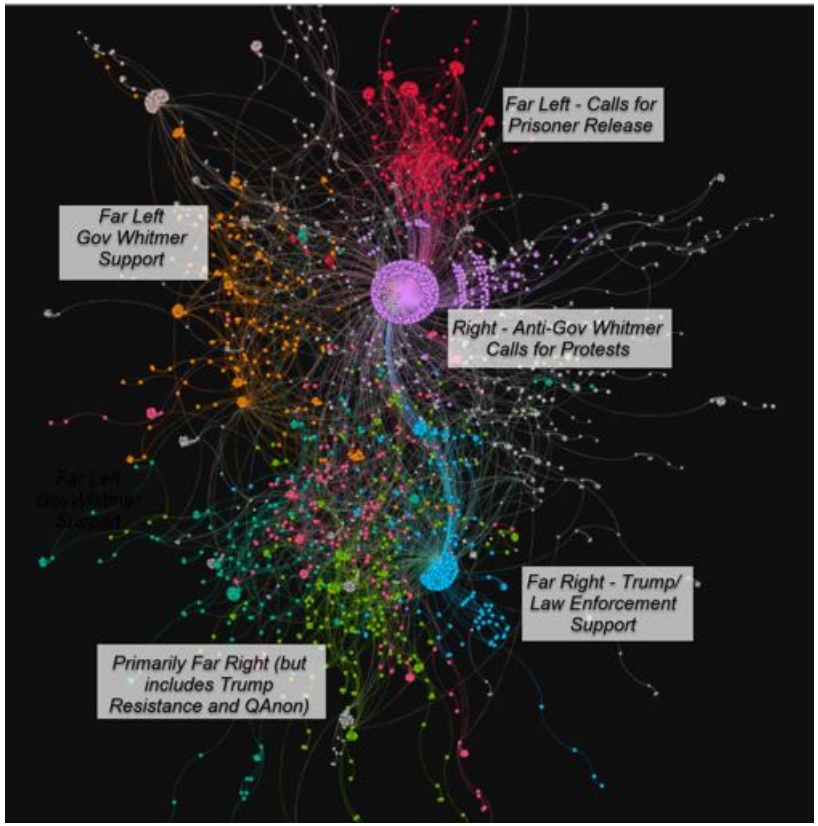
COVID-19 misinformation themes pushed on multiple platforms (blogs, twitter, YouTube, facebook, and other non-mainstream social media platforms). Recurring/periodic themes such as vaccine hesitancy, alternate medicines, conspiracy theories, etc. allow proactive communication strategies and policymaking to detect and mitigate emerging cyber-social threats.



Toxicity analysis on YouTube commenters. Toxic discourse causes disruption and polarization/segregation among communities, as seen above. We demonstrate that by removing highly toxic users from a network, hate speech reduces, online discourse improves, and fractured communities heal. Our findings offer guidance to policymakers within each online social network to make informed decisions about the information environment and derive appropriate and timely countermeasures to continue providing a healthy platform for their users.

Working with LinkedIn and Arkansas Office of the Attorney General

Tracking COVID-19 Misinformation



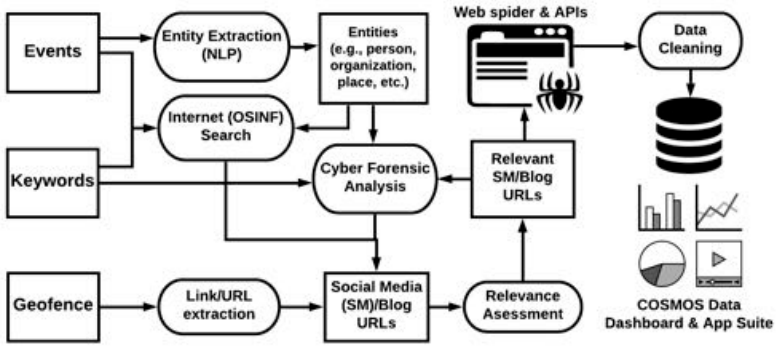
Michigan anti-lockdown protests communication network

- Michigan lockdown protest Twitter data (hashtags: #LetMiPeopleGo, #MiLeg, #Endthelockdown, #MichiganProtest)
  - April 1 to May 20
  - 16,383 Tweets
- Anti-lockdown communication network in Michigan
  - 3,632 nodes
  - 382 groups (focused on 5 most powerful groups)
- FSA/DCFM model showed powerful coordination among far-right twitter groups including QAnon calling for protest and actions against Gov. Whitmer as compared to far-left groups. FBI later unraveled a far-right wing plot to kidnap Gov. Whitmer.

Data Collection & Processing

Over 150 GB of data every day consisting of text, images, audio, video, networks, and metadata

Multi-threaded, distributed, resilient, and scalable data collection framework has been developed, evaluated, and deployed.



Methodology

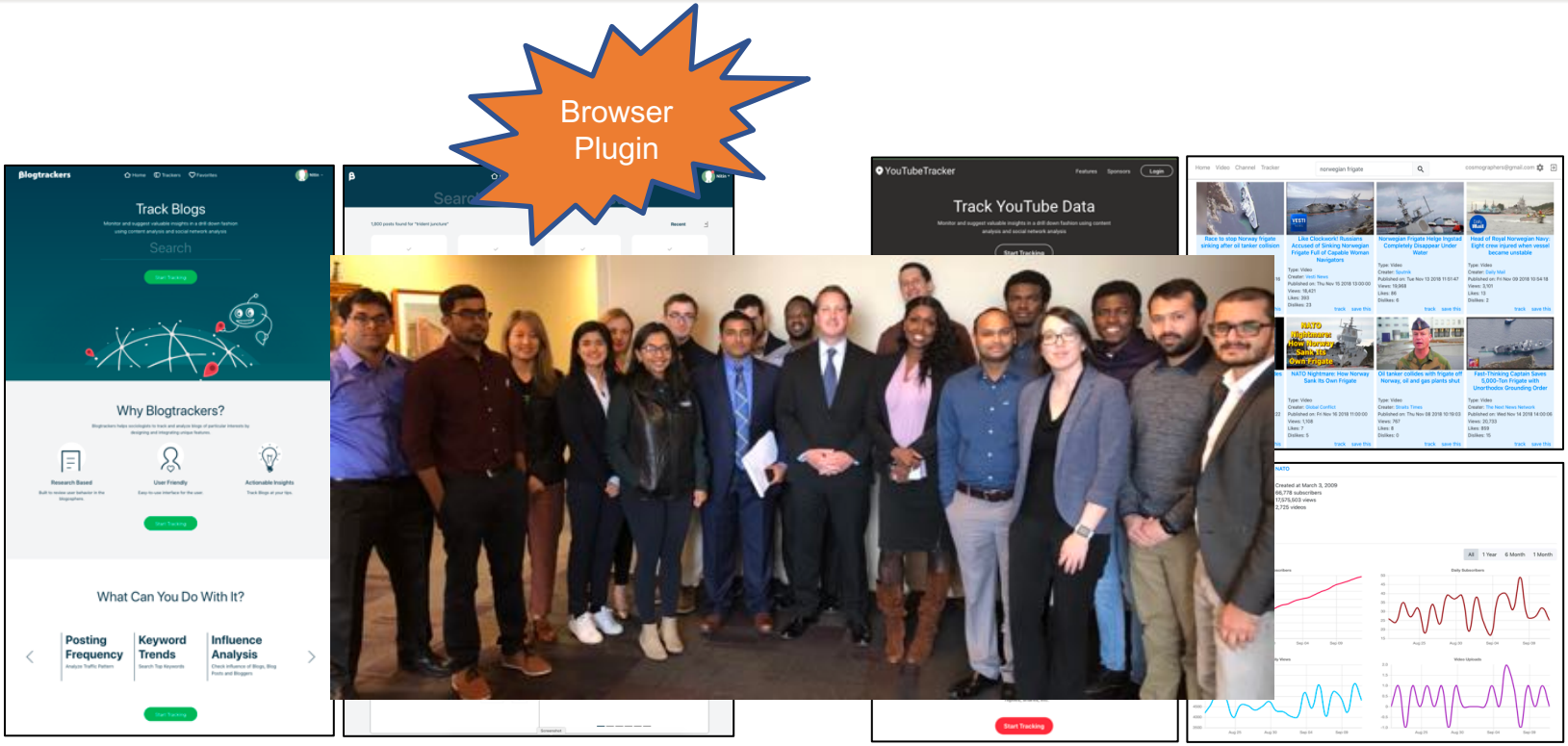
Dashboard

Data Collection & Processing

- Anti-Vaccination discourse
- COVID-19 misinformation
- Indo-Pacific influence campaigns
- NATO's 2015 – 2019 Military Exercises (Trident Juncture, Brilliant Jump, Anakonda, Baltic Operations)
- Canadian 2019 Prime Ministerial Elections
- US 2016 Presidential Elections (e.g., IRA social bot data)
- Migrant crisis (European Union)
- Ukraine and Russia conflict (Euromaidan, Crimean annexation)
- Ukrainian political affairs
- Balkan political affairs
- Venezuelan socio-political crisis

- Blogs
  - 27 attributes
  - 14,854 blog sites, 3,243,408 posts, and 13,794,757 comments
- Twitter
  - 24 attributes
  - 281,546,290 tweets and 42,624,095 users
- YouTube
  - 60 attributes
  - 9,778 channels, 440,950 videos, 160,638,256 comments, 107,551,703 likes/dislikes/views, and 11,563,003 related videos
- Alternate platforms
  - BitChute, Parler, Rumble, Gab, etc.
  - 24 attributes
  - 2,723,790 posts and 38,490,624 views/likes

Technologies Developed



Blogtrackers
btracker.host.ualr.edu/

YouTubeTracker
vtracker.host.ualr.edu/

Selected in US Department of State Global Engagement Center's Tech Innovation program

Social Media Training Course

- III-Marines Expeditionary Force Information Group (III-MIG). July 2020
- NATO Strategic Communications Center of Excellence. 25-29 March 2019. Latvia
- Marine Expeditionary Forces (2MEF). 28-31 August 2018 at CMU, Pittsburgh.
- NATO Strategic Communications Center of Excellence. 20-25 March 2017. Latvia.
- US CyberCommand's CyberSchool, 3-6 August 2016. Ft. McNair

Social Cyber Security Working Group

- Supported by NSF Big Data program
- Over 50 member institutions worldwide including researchers, policy makers, journalists, cyber security professionals
- Outcomes of the working group include
  - Policy briefs laying out the research agenda
  - Collective catalog of resources to spark innovation among researchers

Social Computing Conference, Washington D.C.

- Social Computing, Behavioral-Cultural Modeling and Prediction Conference, Washington D.C., July 6-9, 2021. (over 200 participants)

- Supported by several federal funding agencies.

- http://sbp-brims.org/

Looking Ahead

- Develop publicly available technologies and solutions
- Social media companies need to be more proactive, Algotransparency.org
- Emerging technologies like blockchain for content validation, decentralized social media platforms
- Build collaborative networks of practitioners, researchers, policy makers to address this problem together
- Strengthen media literacy programs
- Need to advance the dialog on cyber diplomacy

Thank you!

Nitin Agarwal, nxagarwal@ualr.edu

COSMOS Tools Developed:

- **COVID-19 -** https://cosmos.ualr.edu/covid-19
- **Blogtrackers** - https://btracker.host.ualr.edu/
- **YouTubeTracker** - https://vtracker.host.ualr.edu/
- **Focal Structure Analysis** - http://fsa.host.ualr.edu/

Blogtrackers YouTubeTracker

FOCAL STRUCTURE ANALYSIS

https://cosmos.ualr.edu/

Follow **cosmographers** on

ACKNOWLEDGEMENTS

This research is funded in part by the U.S. National Science Foundation (OIA-1946391, OIA-1920920, IIS-1636933, ACI-1429160, and IIS-1110868), U.S. Office of Naval Research (N00014-10-1-0091, N00014-14-1-0489, N00014-15-P-1187, N00014-16-1-2016, N00014-16-1-2412, N00014-17-1-2675, N00014-17-1-2605, N68335-19-C-0359, N00014-19-1-2336, N68335-20-C-0540, N00014-21-1-2121), U.S. Air Force Research Lab, U.S. Army Research Office (W911NF-20-1-0262, W911NF-16-1-0189), U.S. Defense Advanced Research Projects Agency (W31P4Q-17-C-0059), Arkansas Research Alliance, the Jerry L. Maulden/Entergy Endowment at the University of Arkansas at Little Rock, and the Australian Department of Defense Strategic Policy Grants Program (SPGP) (award number: 2020-106-094). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organizations. The researchers gratefully acknowledge the support.

COSMOS Collaboratorium for Social Media and Online Behavioral Studies

National Science Foundation · Office of Naval Research · Air Force Research Laboratory · Defense Advanced Research Projects Agency · Army Research Office · Department of Homeland Security · Arkansas Research Alliance