A Research Agenda for Disinformation:

How to make progress when computer science is not enough

Global Security Initiative
Arizona State University

Nadya T. Bliss, PhD
globalsecurity.asu.edu
October 21, 2021
Twitter: @nadyabliss

Dr. Nadya Bliss

Executive Director

Global Security Initiative, ASU

Two decades in national security research and development

- At MIT Lincoln Laboratory and Arizona State University
- At both organizations, have always worked on mission-driven, interdisciplinary research

Currently executive director of ASU's hub for defense/security research

- 4 research centers
- 150+ affiliated faculty span 12 ASU colleges
- GSI FY20 research expenditures: >$34M

National service

- Vice Chair of the Defense Advanced Research Projects Agency (DARPA) Information Science and Technology Study Group
- Computing Community Consortium Council Member (Executive Committee)

Summary

- Disinformation is a complex national security challenge that cannot be addressed solely through the development of new technologies and computer science techniques.

- It requires computer scientists to work closely with experts from other areas to develop systemic socio-technical interventions that build on each other.

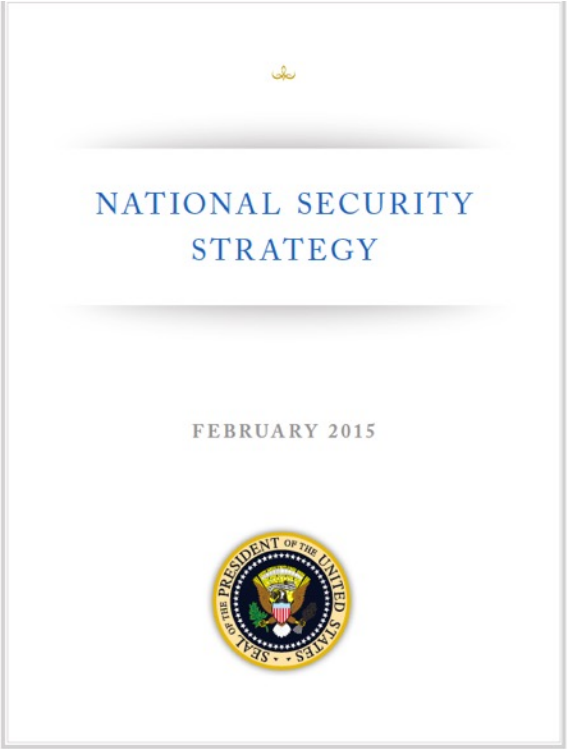
- To adequately address the challenges and security threats posed by disinformation, the U.S. Government, allied nations, and other drivers of large-scale, mission-focused research will need to adjust their standard modality and prioritize truly interdisciplinary research alongside education and training efforts.

- There are some current efforts, but much more needs to be done.

Disinformation: A national security challenge in need of a robust response

From an afterthought to a core national security issue

2015



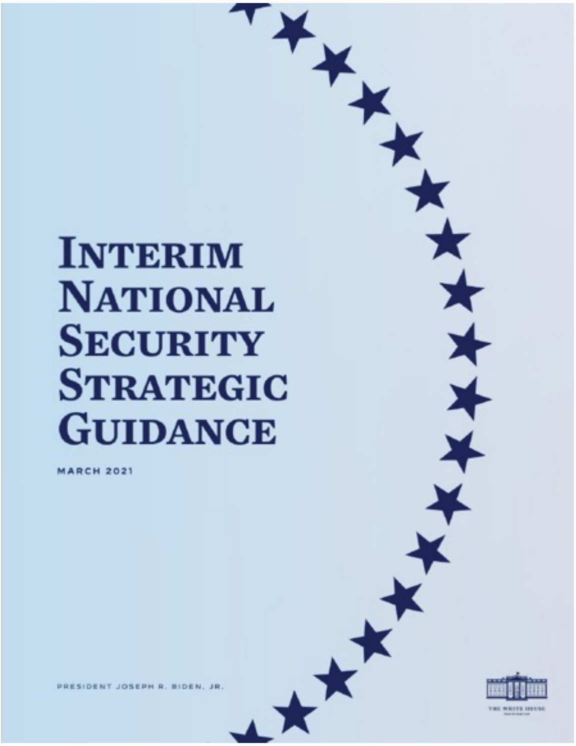
NATIONAL SECURITY STRATEGY

FEBRUARY 2015

Disinformation is not mentioned.

https://history.defense.gov/Portals/70/Documents/nss/NSS2015.pdf?ver=TJJ2QfM0McCqL-pNtKHtVQ%3d%3d

2021



INTERIM NATIONAL SECURITY STRATEGIC GUIDANCE

MARCH 2021

PRESIDENT JOSEPH R. BIDEN, JR.

THE WHITE HOUSE

"Democratic nations are also increasingly challenged from outside by antagonistic authoritarian powers. Anti-democratic forces use misinformation, disinformation, and weaponized corruption to exploit perceived weaknesses and sow division within and among free nations, erode existing international rules, and promote alternative models of authoritarian governance. Reversing these trends is essential to our national security."

https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

Last to know: U.S. government was unprepared for adversarial disinformation efforts

'Information warfare': How Russians interfered in 2016 election

The Propaganda Tools Used by Russians to Influence the 2016 Election

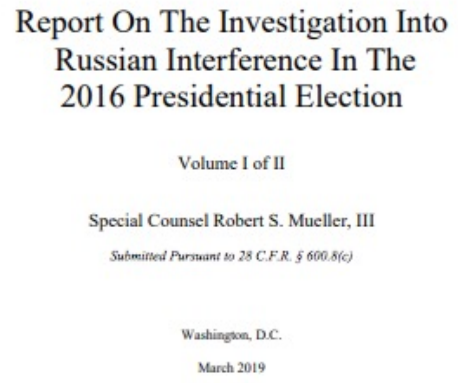
By ALICIA PARLAPIANO and JASMINE C. LEE FEB. 16, 2018

Thirteen Russian nationals have been charged with illegally trying to disrupt the American political process, according to an indictment filed by Robert S. Mueller III, the special counsel investigating Russia's interference in the 2016 presidential election.

Here are the tools the Russians used:

MOLLY MCKEW SECURITY 02.16.18 10:25 PM

DID RUSSIA AFFECT THE 2016 ELECTION? IT'S NOW UNDENIABLE



Report On The Investigation Into Russian Interference In The 2016 Presidential Election

Volume I of II

Special Counsel Robert S. Mueller, III

Submitted Pursuant to 28 C.F.R. § 600.8(c)

Washington, D.C.

March 2019

A response that does not meet the challenge

- The U.S. Government and allies have yet to develop a comprehensive framework for combating such efforts
  - Little investment in new technologies and public education
  - Limited desire for regulation of private sector companies

- Asymmetric value systems leave democracies more vulnerable to information manipulation
  - Prioritize and protect free speech and open communications
  - Fearful that government regulation of new industries will limit innovation

- Industry focuses primarily on functionality and convenience, to the detriment of security
  - Market dynamics motivate industry to want to work geopolitical competitors and adapt business practices as necessary

NEED: A more robust R&D posture toward current and emerging security challenges

1. Increase funding levels
   - In 1960s, U.S. Govt. accounted for nearly twice as much R&D funding as industry. Today, industry funds nearly twice as much R&D as U.S. govt. (Congressional Research Service: *U.S. Research and Development Funding and Performance: Fact sheet*, June 29, 2018)

2. Prioritize truly interdisciplinary research
   - Establish new frameworks for measuring success that go beyond technological requirements

3. Institutionalize a process for exploring potential abuse of new technologies
   - Process should be conducted in concert with development of new technologies

4. Increased resources for public education on new technologies and potential abuses

Precedent: Sputnik and the ‘space race’

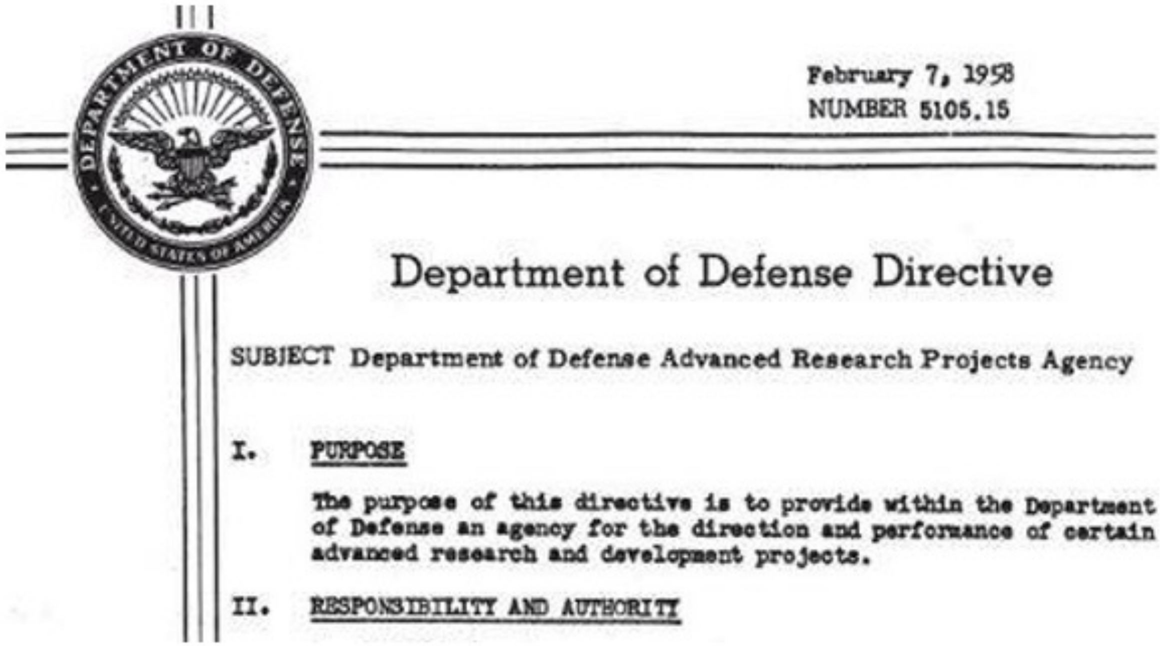
Credit: NASA

- Sputnik: the first artificial satellite, launched by the Soviet Union in October 1957
- Marked the start of the space age and the US/USSR space race
- Sparked a period of fear and anxiety in the U.S. about a perceived technological gap between the U.S. and its Cold War rival, the USSR

American response to Sputnik

Within a year of Sputnik's launch, the U.S. government:

- Created NASA
- Greatly expanded federal funding for STEM education
- Established the first federal student-loan program
- And, created ARPA (later renamed DARPA) to advance military technology



February 7, 1958
NUMBER 5105.15

Department of Defense Directive

SUBJECT Department of Defense Advanced Research Projects Agency

I. PURPOSE

The purpose of this directive is to provide within the Department of Defense an agency for the direction and performance of certain advanced research and development projects.

II. RESPONSIBILITY AND AUTHORITY

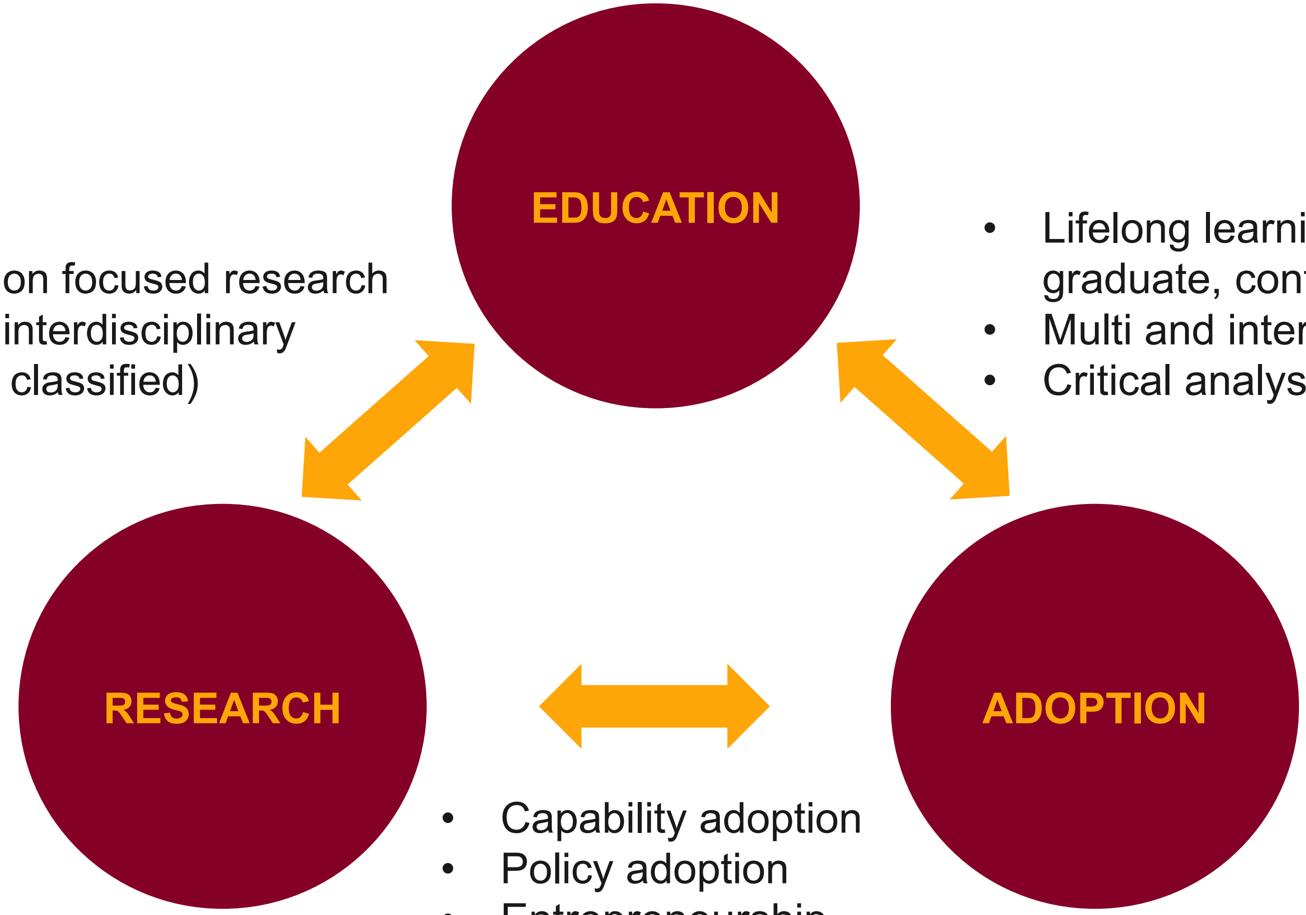
Results of the response

- Established the U.S. Government as a main driver of significant technological advancement over the next few decades
  - Essentially every aspect of information technology on which we rely today bears the stamp of U.S. Govt. support
  - Drove key innovations decades ago
  - U.S. Government support of early-stage scientific research was critical
    - Often took 15 years or more before research translated into a product in the market
    - Developments in one sector often enabled advances in others, sometimes serendipitously
    - Led to the creation of significant business sectors

A path forward

A whole system effort

Education, Research, Adoption and their interaction form the foundation of the systemic response needed to adequately combat disinformation. **Universities must play a critical role in all three components.**



- Basic research
- Mission/application focused research
- Disciplinary and interdisciplinary
- Restricted (IP or classified)

- Lifelong learning (K-12, college, graduate, continuing, non degree)
- Multi and interdisciplinary
- Critical analysis

- Capability adoption
- Policy adoption
- Entrepreneurship
- Social network influence

CCC

Computing Community Consortium
Catalyst

An Agenda for Disinformation Research

A Computing Community Consortium (CCC) Quadrennial Paper

Nadya Bliss (Arizona State University), Elizabeth Bradley (University of Colorado, Boulder), Joshua Garland (Santa Fe Institute), Filippo Menczer (Indiana University), Scott W. Ruston (Arizona State University), Kate Starbird (University of Washington), and Chris Wiggins (Columbia University)

In the 21st Century information environment, adversarial actors use disinformation to manipulate public opinion. The distribution of false, misleading, or inaccurate information with the intent to deceive is an existential threat to the United States—distortion of information erodes trust in the socio-political institutions that are the fundamental fabric of democracy: legitimate news sources, scientists, experts, and even fellow citizens. As a result, it becomes difficult for society to come together within a shared reality; the common ground needed to function effectively as an economy and a nation.

https://cra.org/ccc/wp-content/uploads/sites/2/2020/11/An-agenda-for-disinformation-research.pdf

"The digitization of information exchange, however, also makes the practices of disinformation **detectable,** *the networks of influence* **discernable***, and suspicious content* **characterizable.***"*

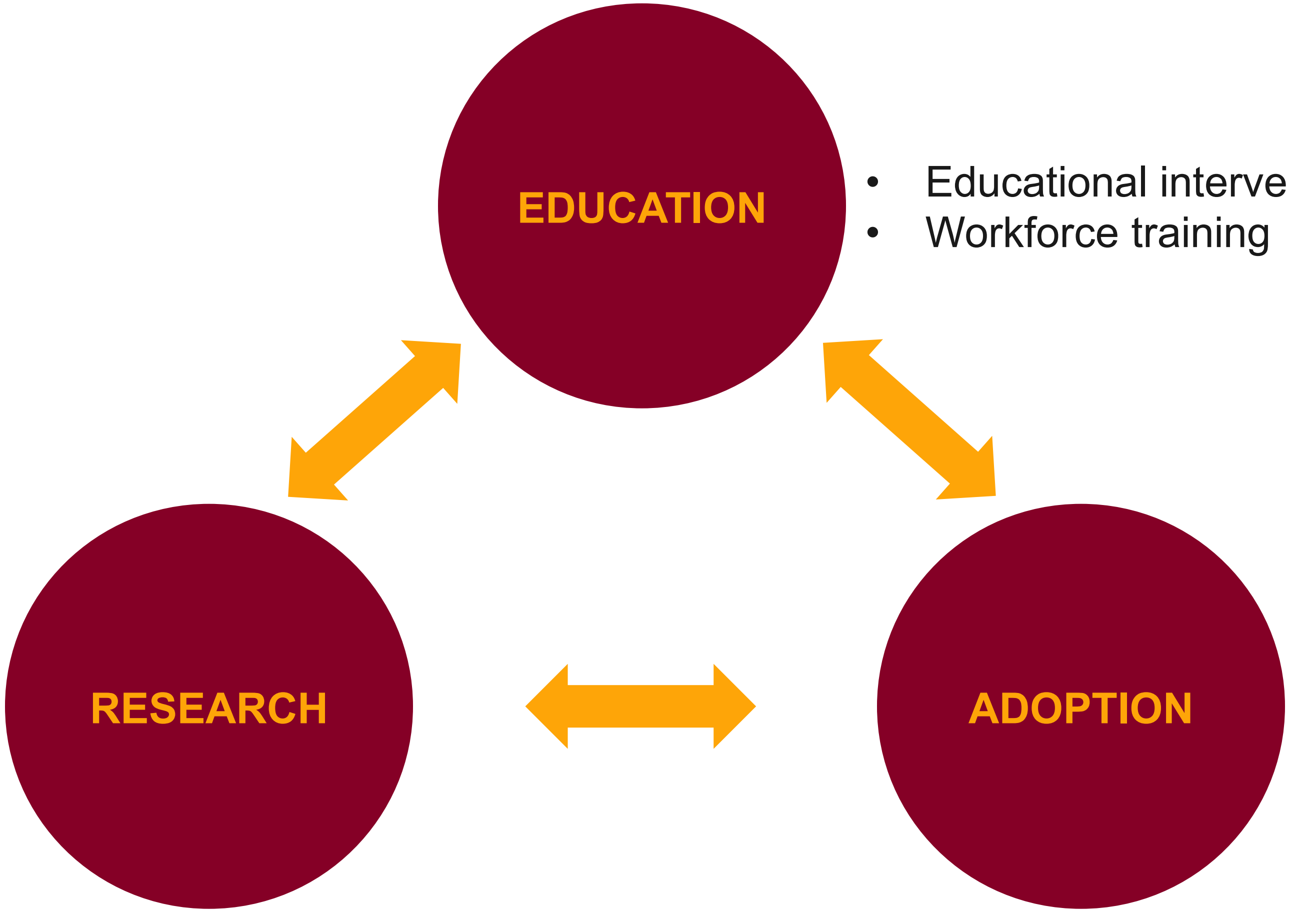
Investments needed in research and interventions in the below areas, with a truly interdisciplinary approach

“This important and ambitious agenda will require a blend of humanities, social science, education, journalism, and computer science…”

1. Detection of disinformation at scale
2. Measurement of impact
3. Data infrastructure
4. New ethical guidelines
5. Educational interventions
6. Workforce training

A whole system effort

Education, Research, Adoption and their interaction form the foundation of the systemic response needed to adequately combat disinformation. **Universities must play a critical role in all three components.**



- Educational interventions
- Workforce training

- Detection of disinformation at scale
- Data infrastructure

- New ethical guidelines
- Measurements of impact

Research

Detection of Disinformation at Scale

“Disinformation and manipulation are adversarial challenges, so both the types of abuse and the methods for detecting them will continue to evolve in the foreseeable future.”

Research efforts directed at:

- Detection
- Provenance
- Attribution
- Integrity
- Verification

Requires targeted advances in:

- Knowledge graphs
- The semantic web
- Machine learning
- Networking
- Data science

Research

Measurement of Impact

“Research is needed to measure the impact of disinformation in different cultural and geographic contexts, over long periods of time, and taking into account second-order effects on social norms, ideologies, epistemologies and sociotechnical structures (like algorithms and social networks) that mediate these impacts.”

Will require advances in:

- Identification and extraction of complex cognitive/rhetorical structures (metaphors, narratives, etc.).
- Development of enduring laboratory proxies of human community engagement – an experimental ‘sandbox’.

Research

Data Infrastructure

“We need a common research infrastructure to access data from technology platforms under ethical guidelines that protect user privacy and transparent administrative rules that protect intellectual property.”

- Different platforms should provide researchers with comparable APIs to enable cross-platform analysis.

- New incentives for platforms and researchers to collaborate across institutions and fields.

- Development of protocols and large-scale infrastructures that allow citizens to contribute data for research in a secure and privacy-preserving manner.

Intervention

New Ethical Guidelines

“Any experimental research aimed at detecting and characterizing disinformation requires gathering of data about real individuals and their communications. In this, the privacy of those individuals must be respected and potential harms must be anticipated.”

- Ethical standards and practices of human subject research currently guided by 1978 Belmont Report, with Institutional Review Boards sometimes interpreting guidelines inconsistently.

- Direct example: is public Twitter content subject to privacy protections?

- Recommendation: Policymakers commission a report of similar impact to the original Belmont report, updating how its principles should be interpreted in light of today’s disinformation ecosystem.

Research/Intervention

Educational Interventions

“Detection efforts are important interventions on the supply side of disinformation. On the demand side, we need to better prepare our citizens for dealing with the modern, computationally accelerated and algorithmically driven information environment.”

- Need broad educational initiatives that raise the level of fundamental knowledge about the information environment to enable citizens to adequately function in civil society.
- Will require research at the intersection of psychology, sociology, philosophy, and the computer and information sciences.
- Need to develop tools that journalists, scientists, and educators can leverage to underpin credible information.

Intervention

Workforce Training

“Much of the technology that is being blamed today for disinformation and manipulation was developed with benign intent and initially brought significant benefits. Its negative repercussions and weaponization were not foreseen by the technologists who developed it.”

- Need the next generation of computing principles to operate with a practicable mindset and toolset for applied ethics.

- Policymakers and research funders sit at a unique point in terms of both perspective and impact in this conversation.

- Development of a shared, useful vocabulary and conceptual toolkit for recognizing and facing future ethical challenges.

Tips and observations from a career in interdisciplinary research

1. The best interdisciplinarians have disciplinary depth and know when they are out of it.
2. Large scale interdisciplinary projects are about more than your research.
3. Team dynamics are just as important as technical expertise.
4. Leadership is vital.
5. As are management and administration.
6. Incentive structures matter.
7. Organizational structures matter too.
8. Diversity of disciplinary cultures is a strength.
9. Patience is key.
10. It is worth it.

> **(The Defense Laboratory System) can't concentrate just on the glamorous, the high-tech, the cutting edge. It must also maintain our superiority in the mundane…**
>
> **Dr. Anita K. Jones**
> **Director of Defense Research and Engineering**
> **Statement to the Senate Armed Services Subcommittee**
> **April 22, 1994**

First presented as keynote at National Science Foundation *Leap to Large* workshop. *May 19, 2021*

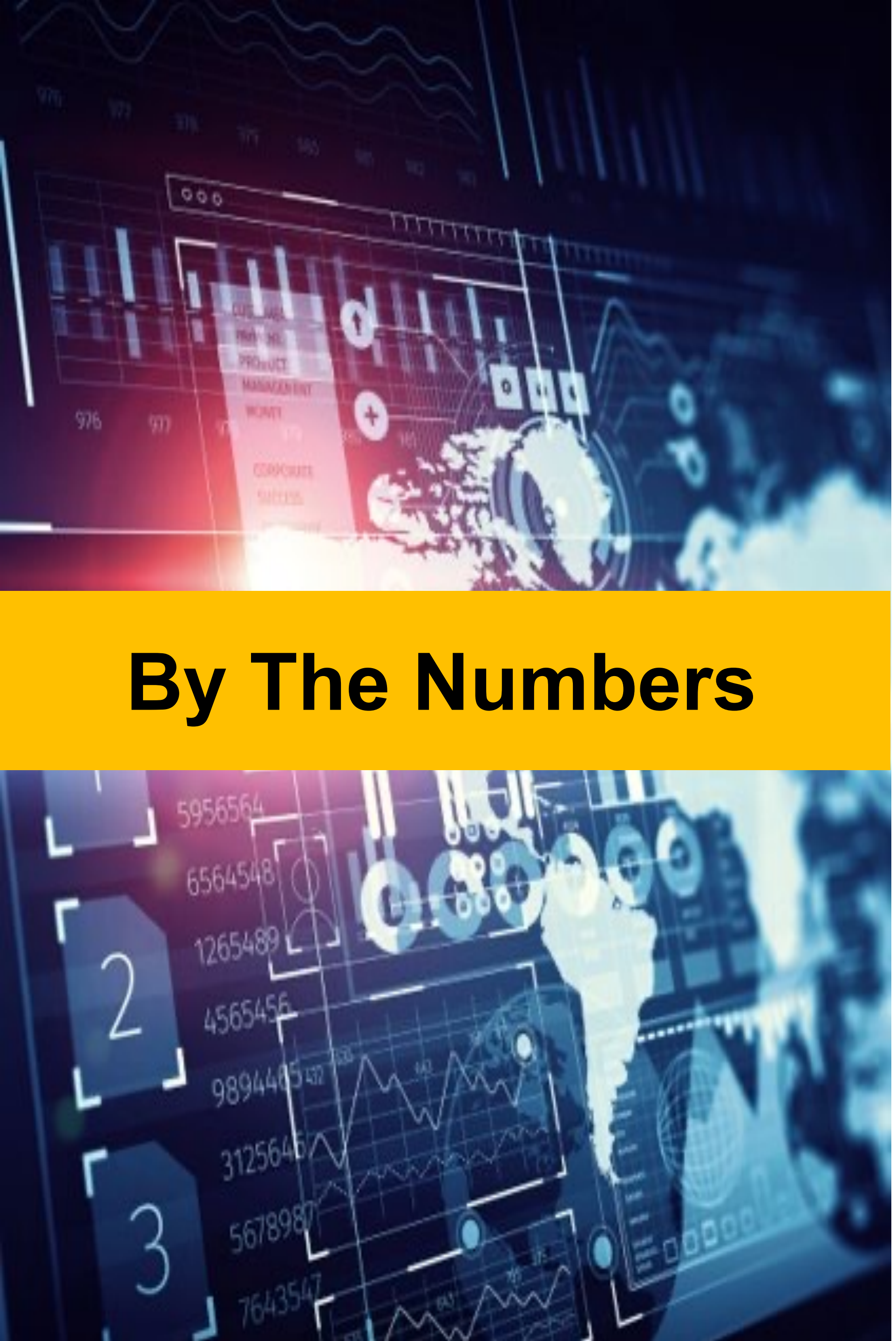
Some current efforts at ASU

ASU Global Security Initiative
Arizona State University

Center on Narrative, Disinformation & Strategic Influence

The Center conducts timely, critical research that fuses the humanities and social sciences with state-of-the-art computer science and modeling in order to develop better insights into how information influences human behavior and geopolitics.

This interdisciplinary research provides evidence-based, mission-relevant insights and tools, benefiting national defense and other stakeholders and their efforts to safeguard the United States, its allies, and democratic principles.



By The Numbers

5 projects currently in execution:

- *DARPA:* Semantic Information Defender
- *DoD Minerva*: Fusing Narrative and Social Cyber Forensics to Understand Covert Influence
- *ONR*: Detecting and Tracking Adversarial Framing in Mainstream and Social Media
- *DHS:* Harmful Narrative Alignment Patterns in the United States
- *MIT Lincoln Lab:* Designing Effective Intervention Points for Adversarial Influence Operations

… totaling $4.9 Million in awards, alongside:

12 universities and 5 industry partners on active, applied or awarded grants.

And, **20+ active members** of the Disinformation Working Group from across ASU with experts in media/journalism, communication, computer science, AI, big data, & more.

Center on Narrative, Disinformation and Strategic Influence

Photo credit: U.S. Navy

Rear Admiral Scott Ruston, Center Director and Research Professor

U.S. Navy: Deputy Commander, Naval Education and Training Command

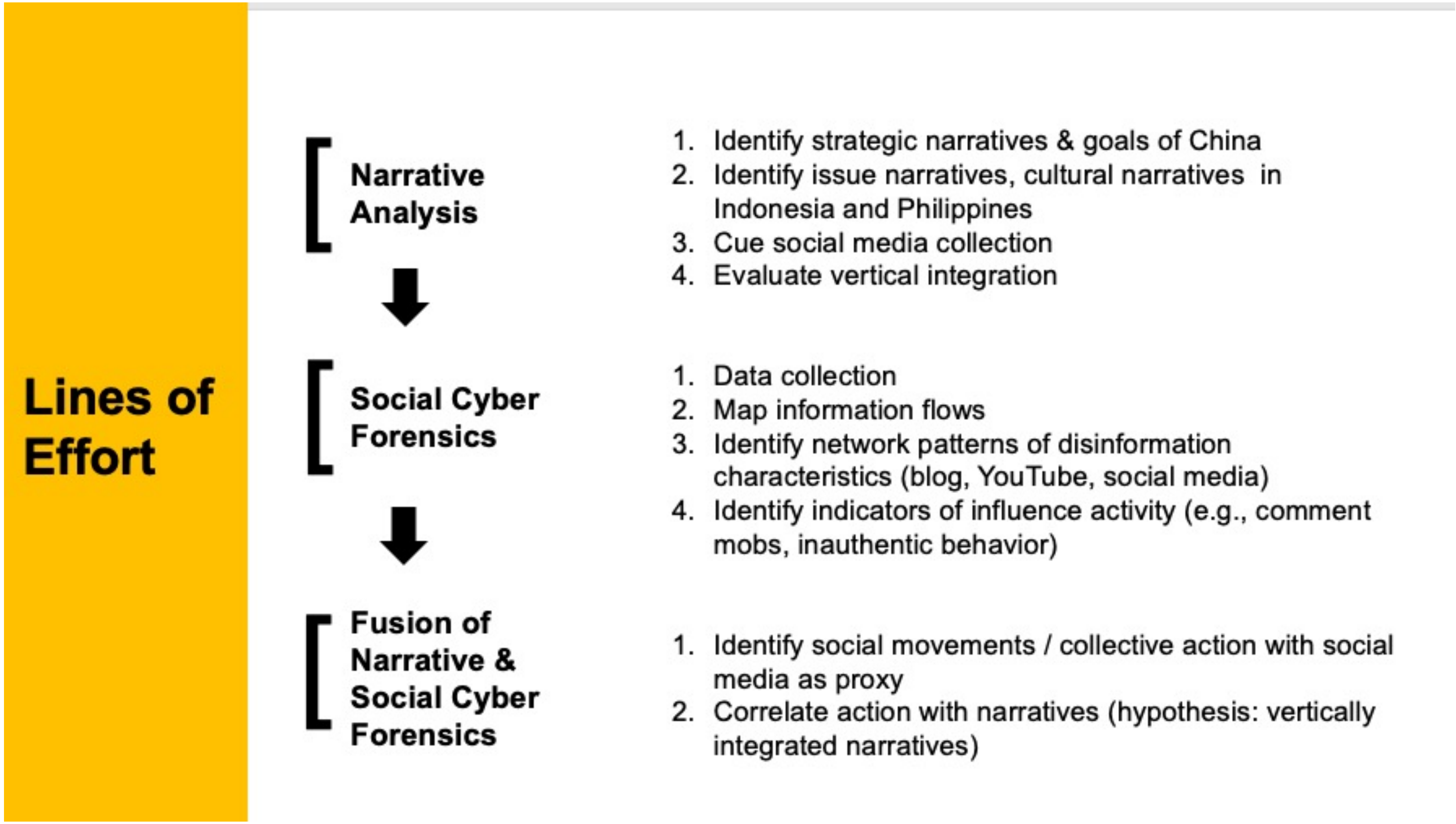
- Expertise in narrative theory and media studies
- Research focuses on the socio-cultural dimensions of the information domain
- Leads research teams that combine humanities, social science and computer science in order to better understand manipulations of the information environment and develop technologies to identify malign influence activities
- Leads ASU's Disinformation Working Group, a collection of ~25 experts from academic units and research units across the university working on the issue of disinformation

Selected publications:

- *Corman, Steven R., Scott W. Ruston, Hanghang Tong (forthcoming 2019).* ***"Toward Generative Narrative Models of the Course and Resolution of Conflict"****. In Social-Behavioral Modeling for Complex Systems, Angela O'Mahoney and Paul Davis, eds. (Hoboken, NJ: Wiley-Blackwell.)*
- *Bernardi, Daniel, Pauline Hope Cheong, Chris Lundry and Scott W. Ruston. (2012)* ***Narrative Landmines: Rumors, Islamist Extremism & the Struggle for Strategic Influence.*** *(Piscataway, NJ: Rutgers University Press).*

Dept. of Defense project: Fusing Narrative and Social Cyber Forensics to Understand Covert Influence

Description: This project maps the information environment and flows of online influence, brings together narrative analysis with social cyber forensic analysis to understand influence campaigns, their appeal, and their calls to action.



Lines of Effort

Narrative Analysis

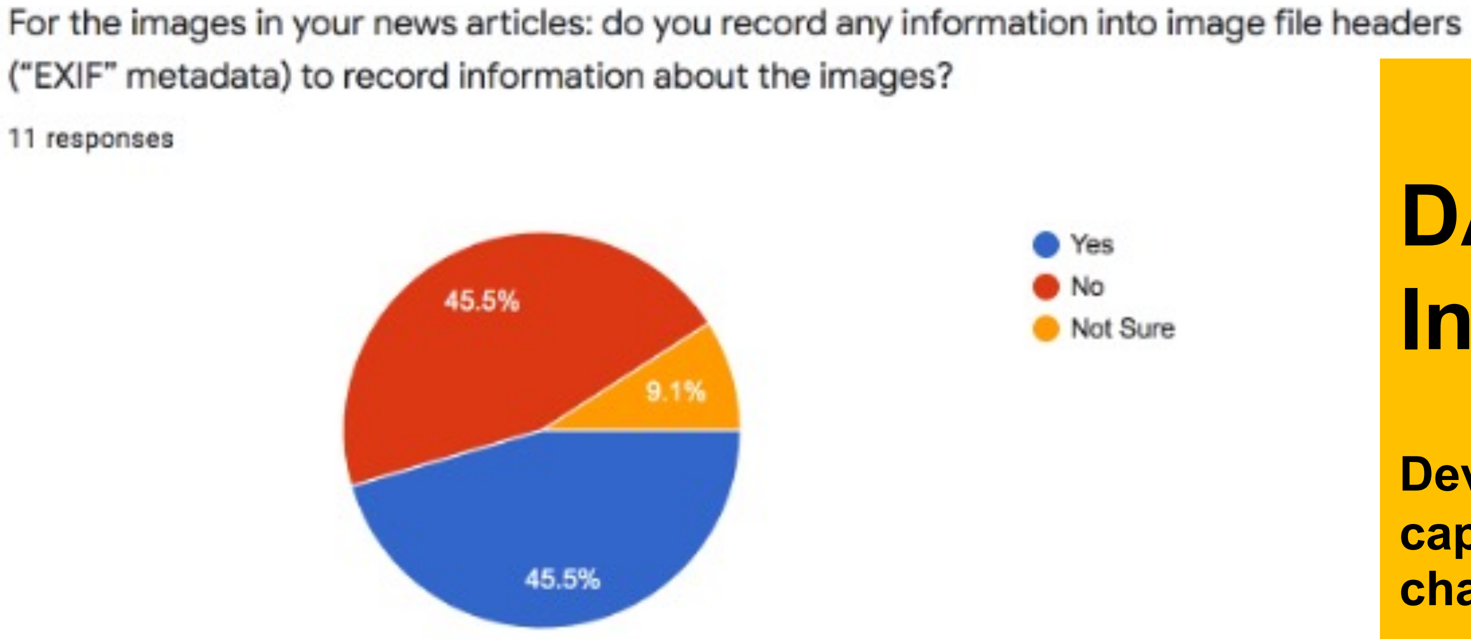
1. Identify strategic narratives & goals of China
2. Identify issue narratives, cultural narratives in Indonesia and Philippines
3. Cue social media collection
4. Evaluate vertical integration

Social Cyber Forensics

1. Data collection
2. Map information flows
3. Identify network patterns of disinformation characteristics (blog, YouTube, social media)
4. Identify indicators of influence activity (e.g., comment mobs, inauthentic behavior)

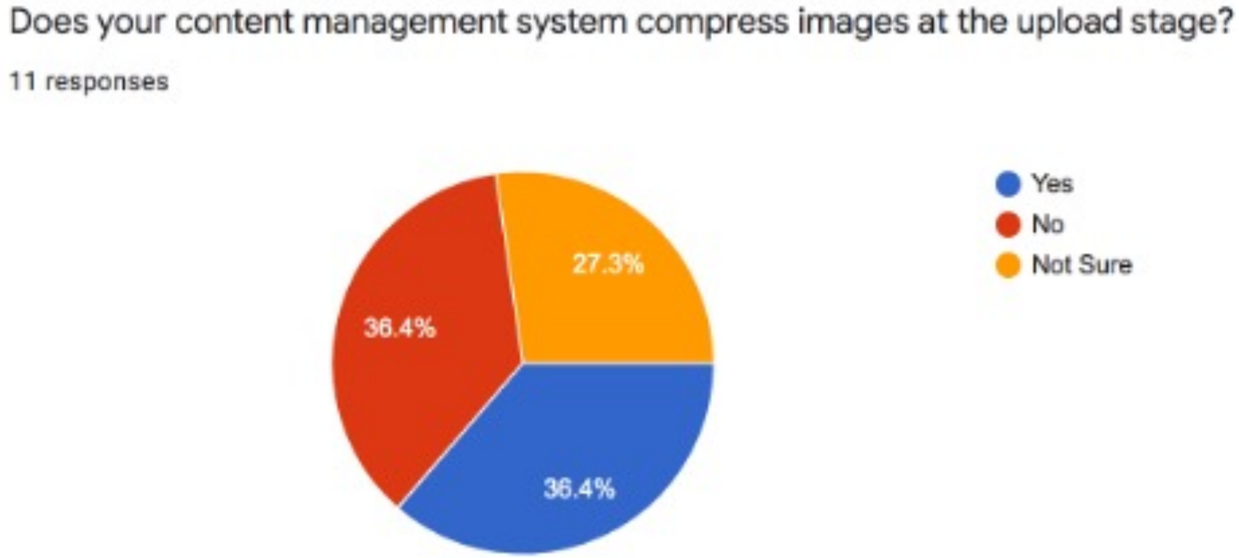
Fusion of Narrative & Social Cyber Forensics

1. Identify social movements / collective action with social media as proxy
2. Correlate action with narratives (hypothesis: vertically integrated narratives)



For the images in your news articles: do you record any information into image file headers ("EXIF" metadata) to record information about the images?

11 responses



Does your content management system compress images at the upload stage?

11 responses

Roschke, K., & Gillmor, D. 2021.

DARPA Semantic Information Defender

Developing a suite of automated capabilities to detect, attribute and characterize manipulated media.

Computer scientists working closely with journalists and others

Research question:

How do you incorporate real-world journalistic practices into a defense-focused technological solution?

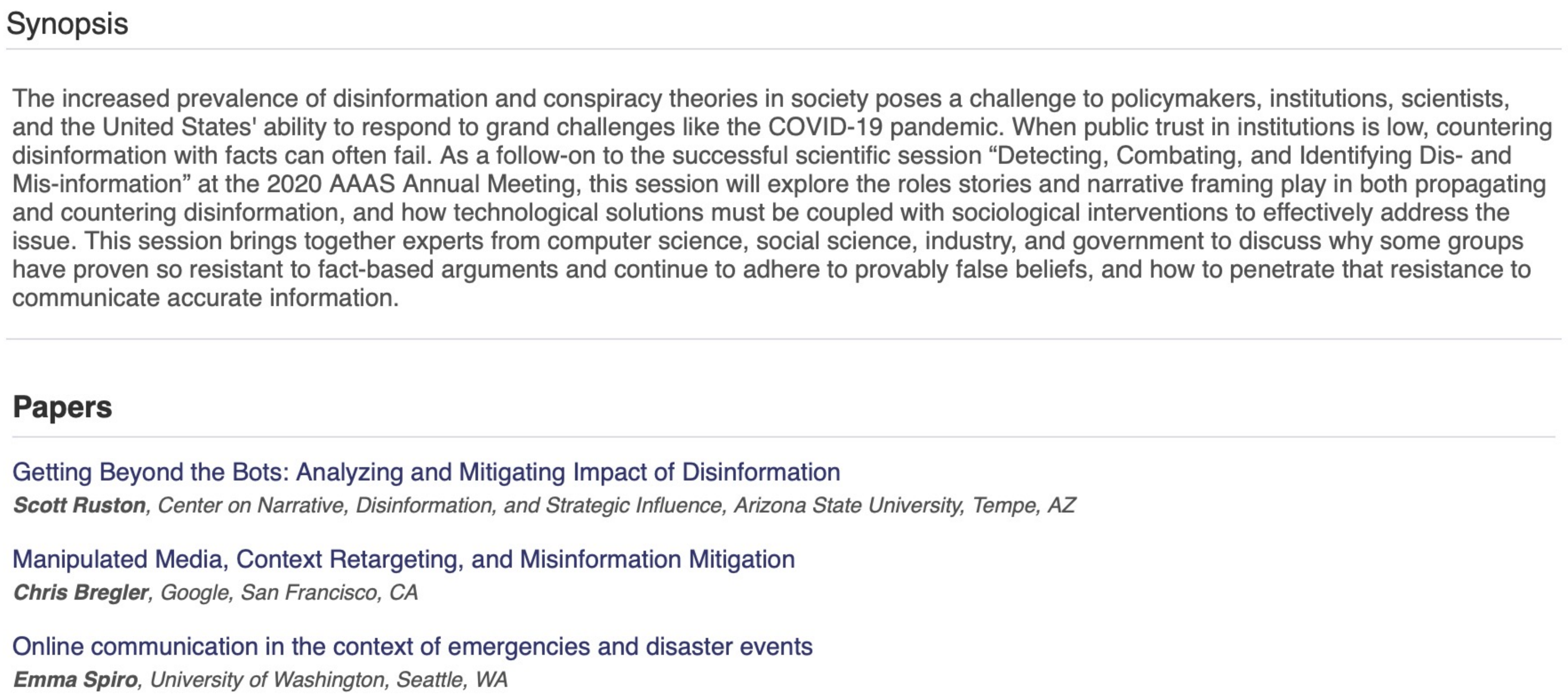
Conclusion

- The spread of disinformation is a serious national, human and cognitive security challenge that is directly impacting the health and well-being of people and the effectiveness of democratic institutions.

- But is not an intractable problem. There is a path toward a world in which disinformation is identified early, kept from spreading widely, and fact-checked and corrected quickly.

- This is only possible if computer scientists, journalists, social scientists and others work together in the research and implementation phases

If you are at AAAS Annual Meeting



Synopsis

The increased prevalence of disinformation and conspiracy theories in society poses a challenge to policymakers, institutions, scientists, and the United States' ability to respond to grand challenges like the COVID-19 pandemic. When public trust in institutions is low, countering disinformation with facts can often fail. As a follow-on to the successful scientific session “Detecting, Combating, and Identifying Dis- and Mis-information” at the 2020 AAAS Annual Meeting, this session will explore the roles stories and narrative framing play in both propagating and countering disinformation, and how technological solutions must be coupled with sociological interventions to effectively address the issue. This session brings together experts from computer science, social science, industry, and government to discuss why some groups have proven so resistant to fact-based arguments and continue to adhere to provably false beliefs, and how to penetrate that resistance to communicate accurate information.

Papers

Getting Beyond the Bots: Analyzing and Mitigating Impact of Disinformation

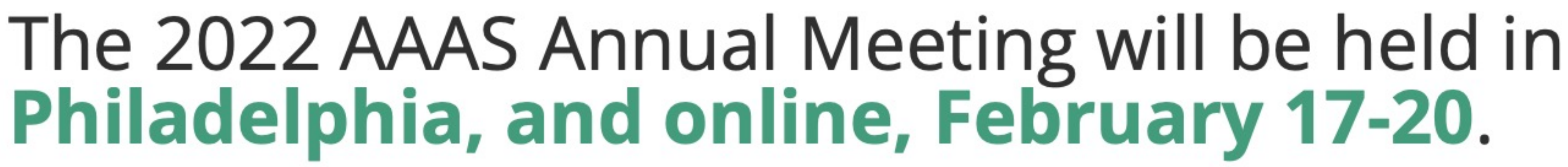
***Scott Ruston**, Center on Narrative, Disinformation, and Strategic Influence, Arizona State University, Tempe, AZ*

Manipulated Media, Context Retargeting, and Misinformation Mitigation

***Chris Bregler**, Google, San Francisco, CA*

Online communication in the context of emergencies and disaster events

***Emma Spiro**, University of Washington, Seattle, WA*



The 2022 AAAS Annual Meeting will be held in **Philadelphia, and online, February 17-20**.

Selected publications

- Bliss N., Bradley E., Garland J., Menczer F., Ruston S., Starbird K., & Wiggins C. (2020) An Agenda for Disinformation Research. https://cra.org/ccc/resources/ccc-led-whitepapers/#2020-quadrennial-papers
- Cepurītis, M., Juurvee, I., Keišs, A., Marnot, D., Ruston, S., & Carrasco Rodríguez, B. (2021). Russia's Footprint in the Nordic-Baltic Information Environment 2019/2020. NATO Stategic Communications Centre of Excellence. https://stratcomcoe.org/publications/russias-footprint-in-the-nordic-baltic-information-environment-20192020/24
- Shu K., Li Y., Ding K., Liu H. (2020) Fact-Enhanced Synthetic News Generation. Proceedings of The Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI 2021). http://www.cs.iit.edu/~kshu/files/aaai_news_generation.pdf
- Shu K., Liu H. (2019) Detecting Fake News on Social Media. Morgan & Claypool Publishers.
- Bhattacharjee A., Shu Kl, Gao M., Liu H. (2021) Disinformation in the Online Information Ecosystem: Detection, Mitigation and Challenges. Journal of Computer Research and Development. https://arxiv.org/pdf/2010.09113.pdf
- Alzahrani S., Kim N., Ruston S., Schlachter J., Corman S. (2018) Framing Shifts of the Ukraine Conflict in pro-Russian News Media. 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.