

©2022 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited. Case Number 21-01760-22.



Response of The MITRE Corporation to the NITRD RFI on Federal Priorities for Information Integrity Research and Development

May 15, 2022

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

<<This page is intentionally blank.>>

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs), participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's 8,000-plus employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision-making, technical findings, or policy recommendations.

MITRE has provided unbiased, trusted advice to federal sponsors regarding how to understand and leverage information for decades, across applications both foreign and domestic. Over the past few years, we have also developed partnerships with research leaders in industry, academia, and the nonprofit sector to provide capabilities to prevent, detect, and respond to information integrity challenges. Our primary focus in this space has been on overcoming information integrity issues with likely dangerous outcomes, such as identifying the source or amplification of influence campaigns with divisive or violent intents or efforts to help states spot and overcome incorrect information about election processes and infrastructure.¹ We also have an interest in countermeasure development, especially in ways of increasing societal resilience through means such as inoculation against or prebunking² disinformation, counter-narrative development, and tuning social media platforms to create pro-social cascades.

Introduction

Individuals, organizations, and governments in open societies depend on access to trustworthy information to make good decisions for themselves, their companies, and their societies. The democratization of media and online content production brought about by the increased ubiquity of the internet has had many positive effects, but also has resulted in new challenges, including propagation of *misinformation* (false information), *disinformation* (false information intended to deceive), and *malinformation* (based on true information, but used out of context to mislead, harm, or manipulate)³ – collectively referred to as mis/dis/malinformation in this response.

¹ MITRE SQUINT™ App Helps Election Officials in 11 States Spot Incorrect Election Information. 2020. MITRE, <https://www.mitre.org/news/press-releases/mitre-squint-app-helps-officials-in-11-states-spot-incorrect-election-information>. Last accessed April 29, 2022.

² D. Blackburn. "Policy Wrappers" for S&T Findings. 2022. MITRE, <https://www.mitre.org/sites/default/files/publications/pr-22-1175-policy-wrappers-for-st-findings.pdf>.

³ Mis, Dis, Malinformation. 2022. Cybersecurity & Infrastructure Security Agency (CISA), <https://www.cisa.gov/mdm>. Last accessed April 26, 2022.

The CISA-based mis/dis/malinformation descriptors above include a concept of true versus false information, but in practice most information is usually not that clearly binary. While some items have been proved beyond a reasonable doubt (the day has 24 hours, the Earth is round and revolves around the Sun, etc.), many others have not. Science evolves, conditions change, the same object can look completely different from various perspectives, and results of assessments can vary wildly as the weighting of its various influences are minutely tweaked. Information integrity efforts must therefore not fall into the rabbit hole of trying to determine absolute truths but rather focus on better enabling entities to adequately assess information, determine its relevance, and properly leverage it via critical reasoning.

As public debate increasingly takes place on privately owned platforms, internet governance topics—including how best to understand, share, and react to online harms, appropriate transparency, and what role government might play in convening, coordinating, or providing oversight, regulation, or guidance to diverse stakeholders—form an important backdrop to the research and development needs for information integrity. Because of disagreement among experts on the drivers, impacts, and scale of information integrity problems, as well as the adjacency to politically charged discussions about free speech and data privacy, issues of information integrity must be addressed in an evidence-based, non-partisan, and scientific manner that is nonetheless attuned to the ongoing values-based discussion about what role communication technologies should play in our democratic society to ensure prosperity and security for all. In the spirit and intent of Integrated Deterrence, these measures and the capabilities that enabled them should also be considered in context of our nation’s many allies and partners, who are also challenged with information integrity and are pursuing their own solutions.

We must also be cognizant of related issues that are detrimental to making progress on information integrity. For example:

- Some of the more vocal entities on the issue of mis/dis/malinformation are also prodigious developers or amplifiers of such information themselves.
- There are growing instances of advocacy or political activities that erroneously assess information as false when it doesn’t align with their existing worldview or support their arguments.
- The concept of how to communicate about information integrity issues and activities so that they are accurately understood and embraced by the population remains in its infancy, with the establishment of the Department of Homeland Security’s Disinformation Governance Board providing a recent high-profile example.

Questions Posed in the RFI

1. Understanding the information ecosystem: there are many components, interactions, incentives, social, psychological, physiological, and technological aspects, and other considerations that can be used to effectively characterize the information ecosystem. What are the key research challenges in providing a common foundation for understanding information manipulation within this complex information ecosystem? A common perspective for understanding and investigating the complex information ecosystem will be an important aspect of driving advancement of information integrity. Absent such a

perspective, individual researchers may not fully recognize the various elements that should be considered while scoping their projects, nor the needs of those who will be impacted by the research. Key aspects that need to be included in such a common perspective include:

- Technical matters, such as infrastructure and data
- Motives and incentives
- Tactics, techniques, and procedures (TTPs)
- Attribution
- Spread/diffusion mechanisms (aka “information maneuvers)
- Impact
- Mitigation
- Collaboration (cross-sector, interdisciplinary, and international)

The Department of Defense has taken some aligned initial actions when it added information as a seventh joint function, as the “information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant-actor perceptions, behavior, action or inaction, and support human and automated decision making.”⁴ Additionally, the *DoD Concept for Operations in the Information Environment*⁵ identifies the required capability to characterize and assess the informational, physical, and human aspects of the security environment. These concepts can be incorporated into a government-wide perspective. Additional research challenges in providing a common foundation for understanding information manipulation include:

Terminology. Common terminology is critical for any field’s advancement as it enables every professional to represent, express, and communicate their findings in a manner that is effectively and accurately understood by their peers. While national and international vocabulary standards take time to develop, there is also a National Science & Technology Council (NSTC) precedent for establishing both definitions and directing agencies to consistently use and follow them on a priority science and technology topic.⁶ The same approach could be leveraged here, starting with a collaborative research activity to develop the definitions.

Guidelines for Proper Scoping. Selecting a proper scope for a research project is critically important but can be challenging. While information ecologies (including people, practices, technologies, and values) are experienced locally, they can also have a broader reach that must be considered. For this reason, it is important that researchers define specifically the components of the information ecosystem that they intend to study, how, and to what ends. For example, studying social media issues via one social media platform, in one language, at a single point in time, while at times illuminating, requires contextualization within the larger set of information ecologies in which people interact—online and offline—across the globe. Given that information

⁴ Doctrine for the Armed Forces of the United States. 2017. Department of Defense, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

⁵ Joint Concept for Operations in the Information Environment. 2018. Department of Defense, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf

⁶ In the mid-2000s, the NSTC’s Subcommittee on Biometrics published a “Glossary” document of biometric terms. As part of its formal approval, its parent NSTC Committees also instructed member agencies to follow those definitions in their future activities. Non-governmental entities (mostly) aligned voluntarily as well and this document served as an important input in the development of an international vocabulary standard, which the subsequent *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards* formally required agencies to follow.

ecosystems are vast and complex, it is incumbent on researchers to prudently plan, clearly define the scope and objectives of research, and then develop appropriate data collection and analysis methods, rather than simply beginning with a limited social media dataset out of convenience. Research that produces best practices and guidelines for properly scoping subsequent information integrity research would be helpful.

Data. Information integrity research requires data, which can be difficult to obtain and/or properly scope, and usually comes with personally identifiable information (PII) concerns. For example, social media researchers often use small Twitter datasets for convenience, but patterns identified in research may not accurately extend to other platforms. Differential access to platforms is also a key challenge, producing the effect of greater study on more developer-friendly platforms as opposed to those with the highest penetration and engagement. Creating adequate and appropriate datasets for training (and separately, testing) purposes, and can evolve over time, is needed. Policy on the use of publicly available information (or foreign websites) is also still needed to guide many federal departments and agencies.

Continuous Evolution. Longitudinal monitoring of the information ecosystem is challenging due to the complex nature of the environment (e.g., account attrition and platform migration, signal-to-noise issues), complicating model development and evolution. As a result, academic research on mis/dis/malinformation is often cross-sectional in nature, which limits applicability to use cases such as change detection (e.g., early identification of extremist behavior). Foundational work is needed to support monitoring that is longitudinal, multi-platform, and inclusive of a broad range of online and offline content.

Language and Platform Variance. One of the challenges in developing research that is multi-lingual, multi-platform, and longitudinal has been the wide variance in social media platform terms of service, policies, and practices. At present, there is a lack of transparency about information manipulation prevention, detection, and response efficacy and measurement within and across social media platforms. As a result, there is no cross-platform view of the information ecosystem as-is state for information manipulation research. There is also a lack of incentive for social media platforms to collaborate with external researchers and the federal government on information manipulation countermeasures research, or to increase transparency about the scope of information integrity issues on their platforms, the specific measures in place to prevent or counter those harms, and how those measures are performing over time. Research to overcome these gaps and to develop guidance on how to perform associated information integrity research from a common perspective is needed.

2. Preserving information integrity and mitigating the effects of information manipulation: strategies for protecting information integrity must integrate the best technical, social, behavioral, cultural, and equitable approaches. These strategies should accomplish a range of objectives including to detect information manipulation, discern the influence mechanisms and the targets of the influence activities, mitigate information manipulation, assess how individuals and organizations are likely to respond, and build resiliency against information manipulation. What are the key gaps in knowledge or capabilities that research should focus on, in order to advance these objectives? What are the gaps in knowledge regarding the differential impact of information manipulation and mitigations on different demographic groups?

Information manipulation is going to occur, both intentionally and unintentionally. It even shows up where we'd least expect it: somewhere between 10 and 20 percent of citations in peer-reviewed scientific journals are used to support claims that conflict with the findings of the original paper.⁷ Thus, while efforts to minimize information manipulation can be helpful, efforts to support identifying and overcoming it will need to be a high priority.

In 2021, MITRE surveyed 29 recent mis/dis/malinformation research agendas and workshop proceedings from across academia, government, civil society, and industry, developing a meta-analysis of priority research needs. Themes within this meta-analysis, which summarize research priorities, are listed below. While this document has not yet been published, a pre-publication draft is provided as Appendix A of this RFI response for the NSTC's benefit.

- Data/infrastructure needs
- Attribution
- TTPs
- Motives
- Spread/diffusion
- Impact
- Mitigation
- Interdisciplinary/cross-sector collaboration
- Cross-platform
- Cross-format
- International perspectives

3. Information awareness and education: a key element of information integrity is to foster resilient and empowered individuals and institutions that can identify and abate manipulated information and create and utilize trustworthy information. What issues should research focus on to understand the barriers to greater public awareness of information manipulation? What challenges should research focus on to support the development of effective educational pathways?

Manipulated information is pervasive because it works. The human mind is naturally receptive to information that aligns with one's cognitive biases. Social media makes it easy for everyone to further share this information with likeminded strangers around the world, which is also further promoted and leveraged by politicians, advocacy organizations, and traditional news media. Network theory shows us how information nodes can grow quickly, particularly with the support

⁷ J. West and C. Bergstrom. Misinformation in and about science. 2021. Proceedings of the National Academy of Sciences of the United States of America, <https://www.pnas.org/doi/10.1073/pnas.1912444117>. Last accessed April 29, 2022.

of adversarial network manipulation. Technological solutions to these challenges are complex, while also raising free speech concerns. Overcoming manipulated information in the wild with counterarguments alone isn't a winnable approach due to realities highlighted in the Brandolini⁸ and Finelli internet idioms.⁹ The problem of manipulated information thus can't be solved without addressing the human component.

Two fundamental obstacles to addressing the human component of the manipulated information problem in modern populations are poor critical reasoning skills and a lack of desire to engage with those who hold alternative views,¹⁰ both of which are routinely leveraged by advocacy-driven organizations. While research to overcome these obstacles won't directly solve the information integrity problem, it would provide insights on how to best raise the floor of what is conceivably possible and should thus be prioritized. We also need to recognize that both obstacles are problems that will require a long time to overcome, and thus sustained efforts will be required.

More directly focused lanes of needed research include:

- Cognitive bias and logical fallacy awareness and impact mitigation
- Intervention options and associated implementation considerations
- Novel education and communication approaches, including public-private partnerships, to inform community-level stakeholders
- How to reach citizens who have low critical reasoning skills and/or are unlikely to participate in digital literacy efforts
- How to properly measure the impact of information manipulation awareness efforts in both the short term and long term.
- Systematically defining and evaluating the conditions under which interventions of different kinds produce long-term positive outcomes
- Research to develop guidelines for critical thinking education by grade level in K-12

We should also pursue immediate efforts to help raise awareness and develop the information integrity skills of our population, both because of the urgent need but also to provide study matter for longer-term research. Example activities or other ideas to potentially leverage include:

- DARPA's Social Media in Strategic Communication (SMISC) Program¹¹ goal was to develop a new science of social networks built on an emerging technology base. Through the program, DARPA sought to develop tools to support the efforts of human operators to counter misinformation or deception campaigns with truthful information.

⁸ Brandolini: The amount of energy needed to refute bullshit is an order of magnitude larger than to produce it.

⁹ Finelli: An idiot can create more bullshit than an expert could ever hope to refute.

¹⁰ The State of Critical Thinking 2020. Reboot, https://reboot-foundation.org/wp-content/uploads/docs/Critical_Thinking_Survey_Report_2020.pdf.

¹¹ Social Media in Strategic Communication. 2022. DARPA, <https://www.darpa.mil/program/social-media-in-strategic-communication>. Last accessed May 10, 2022.

- DARPA’s Influence Campaign Awareness and Sensemaking¹² program is developing techniques and tools that enable analysts to detect, characterize, and track geopolitical influence campaigns with quantified confidence.
- Integrate information integrity topics into existing cybersecurity competitions, such as the Air Force Association’s CyberPatriot¹³ program and the National Collegiate Cyber Defense Competition.¹⁴
- Identify existing integrity awareness offerings and make them accessible and easily findable to others, such as:
 - DoD’s Influence Awareness course
 - Programs by USAID and CISA for local populations
 - Topic-specific offerings
- University of Washington course materials, and associated assets, which helps students identify manipulated data usage.¹⁵
- Create an ongoing public prize challenge to identify (and correct) each week’s most noteworthy information manipulation.
- Create a website that highlights ridiculous information manipulations in an amusing manner, akin to an existing website¹⁶ that aims to show that correlation is not the same as causation.

4. Barriers for research: information integrity is a complex and multidisciplinary problem with many technical, social, and policy challenges that requires the sharing of expertise, data, and practices across the full spectrum of stakeholders, both domestically and internationally. What are the key barriers for conducting information integrity R&D? How could those barriers be remedied?

Research That Is Limited or in a Silo

Information integrity research and development requires a multidisciplinary approach. Bringing together a well-rounded team to research the intersection of technical, social, behavioral, and cognitive spaces is critical to making progress in this space. Much ongoing research, however, is performed within individual lanes of interest: technologists are largely interested in the

¹² B. Kellter. Influence Campaign Awareness and Sensemaking. 2022. DARPA, <https://www.darpa.mil/program/influence-campaign-awareness-and-sensemaking>. Last accessed May 10, 2022.

¹³ Cyberpatriot – The National Youth Cyber Education Program. 2022. Air Force Association, <https://www.uscyberpatriot.org/>. Last accessed May 10, 2022.

¹⁴ National Collegiate Cyber Defense Competition. 2022. Collegiate Cyber Defense Competition, <https://www.nationalccdc.org/>. Last accessed May 10, 2022.

¹⁵ Syllabus with links to readings for course Calling Bullshit: Data Reasoning in a Digital World. 2022. University of Washington, <https://www.callingbullshit.org/syllabus.html>. Last accessed April 30, 2022.

¹⁶ T. Vigen. Spurious Correlations. 2022. Tyler Vigen, <http://www.tylervigen.com/spurious-correlations>. Last accessed April 30, 2022.

information layer; societies are interested in the cognitive, social, and behavioral layer; and policy researchers are interested in broader implications.

- Relatedly, much of the blame for recent information integrity concerns has focused on social media; however, less than half of all Americans receive their news from this source¹⁷—and other sources, such as traditional media, are also substantial contributors to this national problem.

Remedy: Federal sponsorship of research activities (as well as related workshops or other events) should prioritize multidisciplinary investigations, and single-disciplinary investigations should still be done within the context of its placement within the developed common foundation for the information ecosystem. While implementing the NSTC’s information integrity R&D strategy, they should similarly ensure interagency collaboration in each agency’s project creation, implementation, assessment, and knowledge/capability transfer.¹⁸⁻¹⁹

Technical

Traditional information mediums—newspaper, radio, and television—operate on a technically static technology base. Internet mediums, however, rapidly evolve. Replicating studies in a technologically fluid environment is very challenging, but is also a key component of scientific evolution and trust in science.²⁰

This fluidity also presents a data standardization challenge. Social media platforms, for example, have various ways of storing and representing data, as well as allowing access to that data, which complicates cross-platform research. These research challenges are further compounded because different populations use different platforms, with divergences driven both by purpose (socializing, shopping, or communicating) and subjects’ age (younger individuals predominantly use different platforms than do older generations).

In the rush to understand how corrupt information spreads online, we believe baseline research related to this field was neglected. “Despite its prominence in the media, the study of disinformation is still in the process of answering definitional questions and hasn’t begun to reckon with some basic epistemological issues.”²¹ This would explain why there are still disagreements about basic concepts and lexicon that are detrimental to a collaborative research environment.

Remedy: There needs to be serious attention devoted to standardizing (or translating) data and language across platforms and mediums within upcoming efforts to establish a common foundation for the information ecosystem. By creating structure on semantics and data, more progress may be made in the actual research space.

¹⁷ M. Walker and K. Matsa. News Consumption across Social Media. 2021. Pew Research Center, <https://www.pewresearch.org/journalism/2021/09/20/news-consumption-across-social-media-in-2021/>. Last accessed April 30, 2022.

¹⁸ D. Blackburn. Interagency S&T Leadership. 2016. MITRE, <https://www.mitre.org/sites/default/files/publications/pr-16-0916-interagency-s-and-t-leadership.pdf>.

¹⁹ J. Mervis. Spy Agencies Team Up with National Academies. 2016. Science, <https://www.science.org/content/article/spy-agencies-team-national-academies>. Last accessed May 1, 2022.

²⁰ D. Blackburn. When and How Should We “Trust the Science”? 2021. MITRE, https://www.mitre.org/sites/default/files/publications/pr-21-1187-when-and-how-should-we-trust-the-science_0.pdf.

²¹ J. Bernstein. Bad News: Selling the Story of Disinformation. 2021. Harper’s Magazine, <https://harpers.org/archive/2021/09/bad-news-selling-the-story-of-disinformation/>. Last accessed May 1, 2022.

Social and Behavioral

In addition to the age-related platform use variances previously discussed, there's also no established way to evaluate the relationship between an individual's online activity and their real-world beliefs or behavior. Socio-cultural expertise is also limited, as R&D has predominantly focused on English-language materials. Also, the nation's polarization doesn't lend itself to large populations being willing to serve as study participants for information integrity research.

Remedy: Targeted research needs to be performed to overcome these barriers.

Adjacent Policies

Existing laws and policies that are themselves important (some barriers exist for a legitimate reason) can unfortunately create barriers for information integrity research, with data and privacy regulations being a prime example. While there have been attempts to leverage privacy-preserving methods to enable data sharing, needed characteristics within the datasets are often lost.

There is currently considerable debate and public awareness of potential first and fourth amendment concerns regarding federal government use of online materials. Recent policy announcements such as the Declaration for the Future of the Internet and DHS's creation of a Disinformation Governance Board can likewise generate concerns of government overreach in today's polarized environment, creating barriers for future federal research on the topic.

Remedy: Existing policies need to be thoroughly examined in the context of future information integrity research, with objectives to create guidelines and associated tools that allow permissible research to take place while simultaneously preserving the objectives of the original policies. Impacts of new policies need to be analyzed before they are established, and communications about these new policies must be both much better for general audiences as well as specifically tailored for this research audience.

5. Transition to practice: how can the Federal government foster the rapid transfer of information integrity R&D insights and results into practice, for the timely benefit of stakeholders and society?

The Intelligence Community has demonstrated an ability to understand adversary information operations. Its iterative approach to implementing new concepts and capabilities could be instructive to broader public efforts and should be studied. Doing so would allow the private sector to sustain and build its disinformation programs, even as the development of new tools continues. The federal government can further help by brokering a public-private information sharing and R&D coordination mechanism to harness knowledge of the private sector while steering government-led research and operational integration.

6. Relevant activities: what other research and development strategies, plans, or activities, domestic or in other countries, including in multi-lateral organizations and within the private sector, should inform the U.S. Federal information integrity R&D strategic plan?

The meta-analysis provided in Appendix A includes references to a range of R&D strategies on this topic that will be useful here. Additionally, the community should study international efforts, results, and best practices to more fully understand the challenges of information integrity and help drive requirements for disinformation identification, diffusion, and attribution. As an example, The Institute for Strategic Dialogue,²² an international organization headquartered in London, works to identify disinformation and other threats to democracy, to combat these threats, and to raise the awareness of governments to the challenge these threats represent. Understanding the views and activities of such organizations regarding the evolution of disinformation, its uses, and its effects can be a powerful adjunct to the development of the technologies our country needs to meet this challenge itself.

7. Support for technological advancement: How can the Federal information integrity R&D strategic plan support the White House Office of Science and Technology Policy's mission?

Since its inception (in the National Science and Technology Policy, Organization, and Priorities Act of 1976), OSTP has been an impactful force on federal—and, indeed, national—S&T activities. While each administration's OSTP has focused on different priorities, its two predominant functions have been consistent:

- **Policy for S&T:** Establish policies for federal S&T activities, help develop federal S&T budgets, and coordinate interagency S&T activities on priority topics.
- **S&T for Policy:** Ensure that S&T aspects are properly understood in other policy deliberations (such as in national security, government management, or economic matters).

Information integrity is an important aspect of both functions, not only in ensuring that OSTP's own activities and messages are proper but in helping overcome false assumptions by policymakers or inaccurate messages by external entities attempting to persuade them.

The federal information integrity R&D strategic plan will help catalyze research on information integrity matters, leading to new technological capabilities and social and behavioral science approaches to help non-experts better assess the messages they see. But these approaches usually are not rapidly or automatically placed into practice on their own. Rather, OSTP will need to actively work to ensure that they are through their own activities and influence. Doing so will not only help set examples for others to follow but also help ensure that OSTP is able to successfully meet both of its predominant functions with scientific integrity.

²² Institute for Strategic Dialogue (ISD). 2022. ISD, <https://www.isdglobal.org>. Last accessed May 10, 2022.

Appendix A – Research Agenda Meta-Analysis

(PRE-PUBLICATION DRAFT)

Introduction and Methodology

We surveyed recent mis- and disinformation research agendas and priorities, as well as related conference and workshop proceedings from across academia, government, civil society, and industry. Our inclusion criteria for relevant materials were as follows: the publication or conference/workshop must be dated 2017 or more recent; the material must address mis- and disinformation research priorities (rather than specific policy or intervention recommendations); and the materials should preferably represent the interests of a group of researchers within a sector, rather than those of a sole lab. In total we reviewed 29 agendas and workshop summaries and identified researchers' key priorities for future work and included 22 here. A full annotated bibliography of included materials is available.

We identified several major themes from the literature which we present below. Direct quotes and citations from the literature are listed in each theme. Each bullet represents a stated research priority, need, or enabler.

Themes

Data/Infrastructure Needs

Infrastructure

- Bliss et al. point to the need for a common research infrastructure to obtain data from technology platforms, while preserving user privacy, following ethical guidelines, and protecting IP (Bliss, et al., 2020).
- A shared social, institutional, and technological infrastructure is necessary to develop datasets for studying the spread of misinformation on social media. This infrastructure can facilitate research and replicability but requires pressuring social media companies to share data (Lazer, et al., 2017).
- Research will continue to be hindered without broader access to historical data and to a wider range of platforms via APIs for Instagram, TikTok, WhatsApp, and YouTube (Pasquetto, et al., 2020).
- APIs are needed to access data relating to deletions, profile changes, 3rd – party application activities, abuse reports, and suspended accounts (Pasquetto, et al., 2020).
- API endpoints to show specific actions platforms take once a message is identified as containing misinformation (e.g., removals, warning labels, downranking) (Pasquetto, et al., 2020).

Data

- There is a need for both expression data (e.g., data corresponding to engagement with content such as likes and retweets) and impression data (e.g., data corresponding to people who read content). Impression data is hidden from researchers; access to this data would enable new research directions in studying both the spread of misinformation and the effectiveness of mitigation techniques (Pasquetto, et al., 2020).

- Demographic data about social media platform users can enable research into the spread, motivations for sharing, countermeasures against, and behavioral impacts of, misinformation (Pasquetto, et al., 2020).
- Fine-grained temporal data is required to characterize networks in which misinformation thrives, enable analysis of the types of events, policies, and technologies that are susceptible to mis/disinformation campaigns, and to aggregate characteristics about the populations that share misinformation (Pasquetto, et al., 2020).
- The research community would benefit from encrypted messaging data (e.g., WhatsApp data), specifically aggregated information about users and uses of the platform, viral and widely spread content, and random samples of names and groups (Pasquetto, et al., 2020).

Attribution

- Identifying who is conducting “social cybersecurity” attacks (Carley, 2020)
- Attribution is listed as one of the goals of detection of disinformation at scale by Bliss et al. (Bliss, et al., 2020)
- Understanding who shares misinformation would offer pathways to design and test interventions (Pasquetto, et al., 2020).
- Politicians, elites, and government officials are major (but understudied) sources of false information (Weeks & Zuniga, 2019).

TTPS

- Identify, track, and assess emerging propaganda and disinformation tactics, technologies, strategies, and patterns used by state and non-state actors to spread disinformation and propaganda across varied regions and cultures (Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center, 2021).
- Increased data access would enable improved characterization of misinformation in real-world contexts (Pasquetto, et al., 2020).
- Researchers are interested in accumulating the requisite data to study, detect, and combat manipulation. In regard to nation-state data, access to all of the organic Russian content from 2016 across various platforms can reveal TTPs and motives. For example, how much content was election related? What was troll behavior like in battleground states and across the nation? (Pasquetto, et al., 2020)
- Better understand strategies of international influence campaigns on target states (Goalsby & Montgomery, 2021).

Motives

- Understand what the perpetrators motive is; why the attack is being conducted (Carley, 2020).
- Understand why people share misinformation (e.g., does exposure to one’s political opponents or allies affect willingness to share?) (Pasquetto, et al., 2020)
- Understand what misinformation is shared with whom and why (Pasquetto, et al., 2020).

- What motivates people to share information in particular when they know that the information is false? (Pasquetto, et al., 2020)
- Researchers can focus on answering underlying questions behind IOs: what are the motives behind a disinformation campaign? Why do people engage with problematic content? (V. Smith, 2020)

Spread/Diffusion

- Tracing and even predicting the spread of an influence campaign, including tracing attackers across multiple social media, monitors that suggest when diffusion is about to explode, peak, and peter out; improve theories of and methods for monitoring diffusion (Carley, 2020).
- Platforms can dampen the spread of information from just a few websites, the fake news problem might drop precipitously; steps by platforms to detect and respond to manipulations from bots and cyborgs will also naturally dampen the spread of fake news (Lazer, et al., 2017).
- Impression data is currently unavailable, but access to fine-grained impression data would allow researchers to measure the true reach of misinformation and could enable prediction of virality and diffusion path of misinformation with greater accuracy (Pasquetto, et al., 2020).
- Implement product design and policy changes on technology platforms to slow the spread of misinformation; researchers should prioritize understanding how people are exposed to misinformation (Murthy, 2021).
- Algorithms prioritize content that has or is expected to have, a high level of engagement. The risk is an overexposure of polarizing and controversial content and underexposure to less emotive but more informative content. Implications for policymaking include requiring online platforms to provide reports to users showing when, how, and which of their data is sold/used (Lewandowsky, et al., 2020).
- Exposure and belief in false information depends a lot on our social connections but we haven't paid much attention to that yet. We don't know the extent to which people are exposed to false information via their social connections or to what effect (Weeks & Zuniga, 2019).

Impact

Quantify the impact/influence/effect of misinformation

- Quantify by short- and long-term impacts through creation of improved measures of impact, such as polarization or mass-hysteria rather than traditional measures of reach such as number of followers, likes, and recommendation. (Carley, 2020)
- Precise, reliable, and validated measurement of the effect or impact of disinformation on communities- this requires formal statistical causal inference on human belief dynamics; requires advances in identification and extraction of complex cognitive/rhetorical structures and experimental sandbox representative of the ecosystem (Bliss, et al., 2020).
- Development of useful metrics of impact on a single and multiple platforms (Goolsby & Montgomery, 2021).

- Quantification of psychological impacts of disinformation/propaganda is a non-trivial challenge (Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center, 2021).
- Further research should be done that measures the impact of inauthentic behavior, better systems for recording these observations would enable this research. In addition, common metrics for measuring inauthentic behavior at scale should be developed (Wright, Stupak, Nikolich, Mattie, & J. Braun, 2020).
- Lack of common research standards are a concern: there is a lack of methods to measure the effects of influence operations (V. Smith, 2020).

Causal models

- Explore measurement, processes, and effects of polarization, particularly affective polarization (whether political, religious, ethnic, or another type). Particularly interested in causal models of polarization driven by informational, environmental, demographic, and institutional factors (Facebook Research, 2021).
- Expand research that deepens our understanding of health information and why it impacts people (Murthy, 2021).
- The research community has not well documented the effects of (or lack thereof) disinformation on outcomes we care about like voting, polarization, the rise of white nationalism, or echo chambers (Weeks & Zuniga, 2019).
- Politicians, elites, and gov officials are major sources of false information: regardless of whether people believe these claims, do members of the public respond to this information with more incivility, by becoming more engaged, or by ultimately becoming more polarized? (Weeks & Zuniga, 2019)

Offline/ "Real World" Influence

- Real-world influence efforts should be studied along with cyber-social efforts to better illuminate how real-world and cyber-world efforts converge, cohere, and amplify one another (Goolsby & Montgomery, 2021).
- Combine real-world study of human behavior with the study of cyber behavior in a diversity of local social contexts, investigating how social media engagement and participation in new social worlds result in the formation of different identities, beliefs, and behaviors that have significant implications for social stability within different systems of government (Goolsby & Montgomery, 2021).
- Consider both "hard influence" (influence that promotes the development of fissures in society) and "soft influence" (constructive, positive narratives and social rewards) (Goolsby & Montgomery, 2021)
- Measure and assess the impact and effect (including secondary effects) of propaganda and disinformation events on US and international audience decision making (Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center, 2021).
- There is a lack of rigorous research in the link between disinformation and resulting sub-optimal behaviors (Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center, 2021).

- Links between online engagement and radicalization remain unsubstantiated by data. Put more investment into understanding the problem, how it's manifesting, where it's manifesting, in order to be strategic (Brookie, Spitalnick, McCord, Rasmussen, & Gillum, 2021).
- Due to the difficulty of measuring 'real world' impact, much disinformation research has focused on spread using readily measurable behavior (clicks, retweets, site visits, etc.) (Colley, Granelli, & Althuis, 2020)
- Look beyond the spread of disinformation online and especially beyond social media, incorporate more diverse news-sharing behaviors, including offline. Focusing online on social media neglects the significance of traditional media and offline communication networks; social and traditional media should not be considered in isolation (Colley, Granelli, & Althuis, 2020).
- Research that explores deterrents to online and offline problematic behavior related to dangerous speech and harmful conflict (Facebook Research, 2021).

Impacts on Subpopulations

- Prioritize understanding how people are exposed to and affected by misinformation and how this may vary for different subpopulations (Murthy, 2021).
- Understanding how people navigate and trust information sources in specific contexts likely requires qualitative sociological and ethnographic research. The more community-specific research is, the better (Colley, Granelli, & Althuis, 2020).
- Understanding how people across different backgrounds, communities, and cultures interact with, are affected by, and decide to promote or share the spectrum of possibly problematic content (Facebook Research, 2021).

Mitigation

Countering and mitigating effects of disinformation through interventions

- Agent-based modeling to assess the relevant impact of interventions (Carley, 2020)
- External randomized control trials (RCT) on social media platforms without interference or involvement from the companies themselves would allow for rigorous research to understand what kinds of interventions are most effective at reducing an individual's propensity to share misinformation, and to what extent does revealing the source of factual interventions affect behavior (Pasquetto, et al., 2020).
- Research exploring the impact of interventions ideally involve randomly assigning users of platforms to various intervention versus control conditions. Specific interventions include labeling news headlines with fact-checking warnings, prompts that nudge users to consider accuracy before sharing, attempts to increase digital literacy, and assessing impact of incorporating layperson accuracy ratings (Pasquetto, et al., 2020).
- How do mitigation tactics such as removal, warning labels, and downranking, affect the way audiences respond to misinformation? (Pasquetto, et al., 2020)
- Which mitigation tactics work best with which audiences or demographics? (Pasquetto, et al., 2020)

- Development of new approaches to counter influence campaigns, including proactive and reactive strategies by U.S. and allies for messaging activities and other cyber-social efforts, as well as economic and other real-world approaches to counter influence (Goolsby & Montgomery, 2021).
- Study phases of disinformation operations to identify where technology-based solutions could be implemented (Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center, 2021).
- Passive fact checking may not be enough; rather we should think about corrective messages as a form of persuasion or social influence- we don't yet know what message features are effective. Applying theories of social influence and persuasion can help by indicating what message elements are persuasive, which sources are credible, and how to reach less attentive audiences (Weeks & Zuniga, 2019).

Building community resiliency to attacks

- Scalable techniques for teaching critical thinking for social media (Carley, 2020).
- Basic research on the characteristics of resilient communities (Carley, 2020).
- What are the necessary ingredients for social information systems to encourage a culture that values and promotes truth? (Lazer, et al., 2017) Educational efforts, sourcing debunking from communities who maintain a shared narrative, use of social pressure, form bridges across communities to foster production of more neutral and factual content, understanding that not all individuals will be susceptible to intervention.
- Need to understand ways in which a common ground for evidence and rules of arguments can be re-established (Pasquetto, et al., 2020).
- Explore the relation between digital literacy and vulnerability to misinformation; including studies of individuals, small groups, and larger communities, but also wider inquiries into factors that shape the context for the user experience online (Facebook Research, 2021).
- Programs to develop digital literacy to identify disinformation in the wild (Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center, 2021).
- Equip Americans with the tools to identify misinformation, make informed choices about what information they share, and address health misinformation in their communities in partnership with trusted local leaders (Murthy, 2021).
- Invest in longer-term efforts to build resilience against health misinformation, such as media, science, digital, data, and health literacy programs and training for health practitioners, journalists, librarians, and others. (Murthy, 2021)
- Strengthen and scale the use of evidence-based educational programs that build resilience to misinformation (Murthy, 2021)
- Establish quality metrics to assess progress in information literacy. (Murthy, 2021)
- Tools for digital literacy, particularly among older generations, may be useful in limiting the spread of inauthentic behavior. (Wright, Stupak, Nikolich, Mattie, & J. Braun, 2020)

- Educate the public on trustworthy digital information: establish a grant program led by the NSF for the purpose of developing a curriculum on trustworthiness of information in the digital age. (Goodman, Carlson, & Bray, 2021)
- The effectiveness of fact-checking and social interventions is questionable; going forward the field aims to identify social factors that sustain a culture of truth and design interventions that help reward well-sourced news. (Lazer, et al., 2017)

Strengthening institutions

- Support efforts to strengthen local reporting in the face of tightening budgets through subsidies for local news outlets and help obtaining non-profit status. (Lazer, et al., 2017)
- Help people understand the rigor that goes into journalism (source gathering, fact checking, no surprises policy). (Goodman, Carlson, & Bray, 2021)
- Government has a responsibility to encourage independent, professional journalism, avoid crackdowns on the news media's ability to cover the news, avoid censoring content and making online platforms liable for misinformation. (West, 2017)
- Understanding how people navigate and trust information sources in specific contexts is critical, and likely requires offline ethnographic research to address community-specific concerns. (Colley, Granelli, & Althuis, 2020)

Interdisciplinary/Cross-Sector Collaboration

- Outreach and collaboration across academic institutions is needed. Currently this is being facilitated in large part by the DoD Minerva program and the Knight foundation (Carley, 2020).
- The next generation of technologists need to be trained in applied ethics so that their processes align with a practicable mindset and toolset (Bliss, et al., 2020).
- Collaboration between conservatives and liberals to identify bases for factual agreement will heighten the credibility of counter-misinformation endeavors (Lazer, et al., 2017).
- Find ways to support and partner with the media to increase the reach of high-quality, factual information.
- Scholarship that proceeds without acknowledging the theoretical framework of propaganda, analysis of ideology and culture, notions of conspiracy theory, and concepts of misinformation and impact, does so to its empirical detriment and makes identifying solutions harder to articulate because the actual problem to be solved is unclear (Anderson, 2021).
- Kenneth Joseph, Nir Grinberg, and John Wihbey have identified broad avenues of future collaboration between technology platforms and the academic community, ranging from frameworks for survey studies, user-level data about misinformation interactions, actions taken by platforms, content curation and moderation algorithms, and access to historical data (Pasquetto, et al., 2020).
- Miriam Metzger and Andrew Flanagin likewise identified areas of collaboration between social media platforms and academic researchers to capture user and network level data.

- Albarracin et al point out that interdisciplinary and intersectoral collaborations between government and social media companies is necessary, particularly when social media companies are not always forthcoming about the information they are spreading.
- Both government and industry have called for social-science-forward approaches to drive the next generation of computational research into quantification of disinformation and its community impacts.
- Facebook has called for collaboration within academic disciplines, with particular attention paid to social science methods, comparative politics and cultural research, and studies that focus on Non-Western measures and analyses (Facebook Research, 2021).
- Topic 4 of the Minerva 2021 research priorities seeks multidisciplinary theoretically innovative approaches from disciplines such as anthropology, cross-cultural sociology, political science, political economy, and cross-cultural social psychology, working in collaboration with computer and information sciences to develop a social-science-forward approach to the development of social theory and the creation of new techniques needed to carry out a systemic analysis of social influence in online and offline cross-cultural milieus, cyber-social dynamics, narrative, and in languages other than English. Particular attention is paid to studies in important strategic regions in Asia, Africa, and Latin America. (Goolsby & Montgomery, 2021)
- Topic 5 of the Minerva 2021 research priorities seeks to involve social scientists, media researchers, area specialists working with information and/or scientists to develop approaches to studying influence of both online and offline communities. (Goolsby & Montgomery, 2021)
- Topic 6 of the Minerva 2021 research calls for new models of collaboration, innovative experimental design, and data analysis to explore computational social science research on difficult-to-access environments. (Goolsby & Montgomery, 2021)
- Global Engagement Center Counter Disinformation and Propaganda center identified primary shortfalls in two areas: understanding the information environment and measuring impact and effectiveness, suggesting that basic capabilities to develop an awareness of propaganda and disinformation may be low, and that there is limited interagency and intergovernmental capability coordination. (Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center, 2021)
- In the U.S. Surgeon General's Advisory on Confronting Health Misinformation (Murthy, 2021), one key area of concern was to convene federal, state, local, territorial, tribal, private, nonprofit, and research partners to explore the impact of health misinformation, identify best practices to prevent and address it, issue recommendations, and find common ground on difficult questions, including appropriate legal and regulatory measures that address health misinformation while preserving user privacy and freedom of expression.
- Funders and foundations are encouraged to move with urgency toward coordinated, at-scale investment to tackle misinformation, and to incentivize coordination across grantees to maximize reach, avoid duplication, and bring together a diversity of experience.

- Government agencies are encouraged to convene federal, state, local, territorial, tribal, private, nonprofit, and research partners.
- Projects and development should be informed by anthropologists, with particular attention paid to differences in ways individuals interact with information. (Wright, Stupak, Nikolich, Mattie, & J. Braun, 2020)

Cross Platform

- Inspect information practices and flows across multiple communication technologies or mediums. In particular, individual, group, and community effects of information campaigns, inauthentic behavior, or coordinated activities across multiple communities, networks, channels, or platforms. (Facebook Research, 2021)
- Platforms should provide vetted researchers with comparable, open APIs to enable cross-platform analytics. (Bliss, et al., 2020)
- Are some types of events, policies, or technologies uniquely susceptible to mis/disinformation campaigns? (Pasquetto, et al., 2020)
- Can we enable research using private encrypted messages, such as those on WhatsApp to track the dissemination of misinformation at scale? (Pasquetto, et al., 2020)
- Cross-platform information ecosystem understanding: research that inspects information practices and flows across multiple communication technologies or mediums. (Facebook Research, 2021)
- Researchers need to look to non-obvious platforms (e.g., Airbnb). (Brookie, Spitalnick, McCord, Rasmussen, & Gillum, 2021)

Cross-Format

- Investigate the role of non-textual media (images, videos, audio, etc.) on the effectiveness of and people's engagement with misinformation. Media types include basic multimedia, simple or advanced manipulated multimedia (deepfakes, cheapfakes), out-of-context imagery, impersonation of public figures/organizations, etc. (Facebook Research, 2021)

International Perspectives

- Comparative research and inclusion of non-Western regions that have experienced a growth in social media platform use: particularly South and Central America, Sub-Saharan and Northern Africa, the Middle East, and Central, South and Southeast Asia. (Facebook Research, 2021)
- Utilize non-Western measures and analyses to study affective polarization, particularly when applied to questions of equitable impact on vulnerable communities. (Facebook Research, 2021)
- Analyze dangerous speech, conflict, and violence in markets with limited institutions, developing media markets, and various levels of democracy in non-Western contexts.
- Research has lagged in studying important strategic regions in Asia, Africa, and Latin America. Multidisciplinary theoretically innovative approaches are needed to carry out systemic analysis of social influence in online and offline cross-cultural milieus and in languages other than English. (Goolsby & Montgomery, 2021)

- Enhance understanding of difficult-to-access environments, such as those experiencing enduring conflicts to societies that broadly restrict researcher access. (Goolsby & Montgomery, 2021)
- Overseas disinformation trends incubate in other countries before coming to the U.S.; likewise, U.S. disinformation exports to other countries (e.g., anti-vaxx content). (Frenkel & Newton, 2021)
- Other countries could use the U.S.'s seizure of Iranian controlled domains as an opportunity to use claims of disinformation to silence dissent. (Frenkel & Newton, 2021)
- The global, long reach of extremism leads to groups finding new issue of the day. (Brookie, Spitalnick, McCord, Rasmussen, & Gillum, 2021)
- Not all disinformation campaigns are aimed at causing violence; some seek to rewrite history. (Brookie, Spitalnick, McCord, Rasmussen, & Gillum, 2021)
- Researchers need to look also at non-Western dominant brand names (e.g., WeChat). (Brookie, Spitalnick, McCord, Rasmussen, & Gillum, 2021)
- Little work is done to understand how governments use influence operations on their own citizens, the role of media in these campaigns, influence in Africa, and non-English language influence operations. (V. Smith, 2020)
- In many countries, few individuals share news on social media, fewer trust it, and the trust is declining. (Colley, Granelli, & Althuis, 2020)
- Study disinformation's impact in a broader range of cultural contexts. (Colley, Granelli, & Althuis, 2020)
- There are 83+ languages in Ethiopia; as of June there was only automated translation available for Amharic (the national language) and neither human or automated translation for any other languages. The platforms could not see/hear/understand the content circulating on their platforms. (Ingrahm, 2021)

References

- Anastasi, J. S., & Rhodes, M. G. (2005). An own-age bias in face recognition for children and older adults. *Psychonomic Bulletin & Review*, 12(6), 1043-1047.
- Anderson, C. (2021, April 15). Propaganda, misinformation, and histories of media techniques. *Harvard Kennedy School (HKS) Misinformation Review*. doi:<https://doi.org/10.37016/mr-2020-64>
- Atlantic Council GeoTech Center & U.S. State Department Global Engagement Center. (2021). Second Counter Propaganda and Disinformation Technology Working Group. unpublished.
- Bliss, N., Bradley, E., Garland, J., Menczer, F., Ruston, S. W., Starbird, K., & Wiggins, C. (2020). *An Agenda for Disinformation Research*. Retrieved from arXiv preprint: <http://arxiv.org/abs/2012.08572>
- Brookie, G., Spitalnick, A., McCord, M., Rasmussen, N., & Gillum, R. (2021, June 22). Fighting online extremism in 'the Klan den of the twenty-first century. Atlantic Council DFR Lab 360/Open Summit. Retrieved from <https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-spot-the-latest-trends-in-digital-disinformation/>
- Carley, K. M. (2020). Social cybersecurity: an emerging science. *Comput Math Organ Theory*, 26, pp. 365-381. doi:<https://doi.org/10.1007/s10588-020-09322-9>
- Colley, T., Granelli, F., & Althuis, J. (2020). Disinformation's Societal Impact: Britain, COVID, and Beyond. *Defence Strategic Communications*, 8. doi:10.30966/2018.RIGA.8
- Facebook Research. (2021). *Foundational Integrity Research: 2021 Misinformation and Polarization request for proposals*. Menlo Park: Facebook. Retrieved August 11, 2021, from <https://research.fb.com/programs/research-awards/proposals/foundational-integrity-research-2021-misinformation-and-polarization-request-for-proposals/>
- Facebook Research. (2021, June 14). Foundational Integrity Research: 2021 Misinformation and Polarization request for proposals. Retrieved August 11, 2021, from <https://research.fb.com/programs/research-awards/proposals/foundational-integrity-research-2021-misinformation-and-polarization-request-for-proposals/>
- Feinman, S., & Entwisle, D. R. (1976). Children's ability to recognize other children's faces. *Child Development*, 47(2), 506-510.
- Fredheim, R., Bay, S., Dek, A., Dek, I., & Singularex. (2021). Social Media Manipulation Report 2020. NATO Strategic Communications Center of Excellence. Retrieved from ISBN: 978-9934-564-92-5
- Frenkel, S., & Newton, C. (2021, June 22). How to spot the latest trends in disinformation. Atlantic Council DFR Lab 360/Open Summit. Retrieved from <https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-spot-the-latest-trends-in-digital-disinformation/>
- Goodman, J., Carlson, T., & Bray, D. (2021). *Report of the Commission on the Geopolitical Impacts of New Technologies and Data*. The Atlantic Council GeoTech Center. Retrieved from ISBN-13: 978-1-61977-178-9

- Goolsby, R., & Montgomery, D. (2021). *FY21 Minerva Research Initiative Topics of Interest*. Minerva Research Initiative. Retrieved from https://minerva.defense.gov/Owl-In-the-Olive-Tree/Owl_View/Article/2069926/it-takes-social-science-to-counter-the-power-of-russias-malign-influence-campai/
- Grother, P. J., Ngan, M. L., & Hanaoka, K. K. (2018). *Ongoing face recognition vendor test (FRVT) part 2: Identification*. Gaithersburg, MD, USA: NIST.
- Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. Gaithersburg, MD, USA: National Institute of Standards and Technology.
- Grother, P., Ngan, M., & Hanaoka, K. (2019). *Ongoing face recognition vendor test (FRVT) part 1: Verification*. Gaithersburg, MD, USA: NIST.
- Ingrahm, M. (2021). What should we do about the algorithmic amplification of disinformation. *Columbia Journalism Review*. Retrieved from https://www.cjr.org/the_media_today/what-should-we-do-about-the-algorithmic-amplification-of-disinformation.php
- Lazer, D., Baum, M., Grinberg, N., Friedland, L., Joseph, K., Hobbs, W., & Mattsson, C. (2017). Combating Fake News: An Agenda for Research and Action. *Combating Fake News: An Agneda for Research and Action*. Cambridge. Retrieved from <https://www.sipotra.it/wp-content/uploads/2017/06/Combating-Fake-News.pdf>
- Lewandowsky, S., Smilie, L., Garcia, D., Hertwig, R., Weatherall, J., Egidy, S., . . . Leiser, M. (2020). *Technology and Democracy: Understanindg the influence of online technologies on political behavior and decision-making*. European Commission Joint Research Centre (JRC). doi:<http://dx.doi.org/10.2760/593478>
- Murthy, V. H. (2021, July 15). Confronting Health Misinformation: The U.S. Surgeon General's Advisory on Building a Healthy Information Environment. Retrieved August 12, 2021, from <https://www.hhs.gov/sites/default/files/surgeon-general-misinformation-advisory.pdf>
- Nothhaft, H., Bradshaw, S., & Neudert, L. (2018). *Government Responses to Malicious Use of Social Media*. Riga: NATO Strategic Communications Center of Excellence. Retrieved from ISBN: 978-9934-564-31-4
- Pasquetto, I. V., Swire-Thompson, B., Amazeen, M. A., Benevenuto, F., Brashier, N. M., Bond, R. M., . . . Flammini, A. (2020, December 9). Tackling misinformation: What researchers could do with social media data. *Harvard Kennedy School Misinformation Review*. Retrieved August 11, 2021, from <https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-could-do-with-social-media-data/>
- Shapiro, P. N., & Penrod, S. (1986). Meta-analysis of facial identification studies. *Psychological Bulletin*, *100*(2), 139.
- V. Smith, N. T. (2020). *Survey on Countering Influence Operations Highlights Steep Challenges, Great Opportunities*. Carnegie Endowment for International Peace Partnership for Countering Influence Operations. Retrieved from <https://carnegieendowment.org/2020/12/07/survey-on-countering-influence-operations-highlights-steep-challenges-great-opportunities-pub-83370>

- Weeks, B., & Zuniga, H. G. (2019). What's Next? Six Observations for the Future of Political Misinformation Research. *American Behavioral Scientist*.
doi:<https://doi.org/10.1177/0002764219878236>
- West, D. (2017). *How to combat fake news and disinformation*. Brookings. Retrieved from <https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/>
- Wright, A., Stupak, P., Nikolich, A., Mattie, K., & J. Braun. (2020). Inauthentic Behavior in Online & Digital Systems Final Conference Report. *Inauthentic Behavior in Online & Digital Systems*. University of Chicago. Retrieved from https://harris.uchicago.edu/files/nsf_report_final.pdf
- Wright, D. B., & Sladden, B. (2003). An own gender bias and the importance of hair in face recognition. *Acta Psychologica*, 114(1), 101-114.