Dancing in the Dark

Disinformation Researchers Need More Robust Data and Partnerships

By Renée DiResta

Beginning in January 2020, researchers who study misinformation and disinformation were afforded the unique opportunity to scrutinize the truly global theme of the new coronavirus and its associated illness, COVID-19. As the disease spread, media began to cover—and social media communities began to discuss—a wide variety of narratives about the virus.

Although the COVID-19 pandemic is not the first major disease outbreak in the era of social media—Zika, Ebola, and measles outbreaks previously demonstrated the ease with which misinformation and conspiracies can spread among impacted communities—it revealed significant vulnerabilities in the global information ecosystem, and made clear the need to improve processes for rapidly detecting and mitigating misinformation. Addressing these vulnerabilities will require multistakeholder, interdisciplinary collaboration.

Slow and unclear communication from health authorities revealed gaps in how authoritative information reaches people in crisis situations, both over social as well as broadcast media; when people are searching for answers and there is no reputable content to return, bad information may fill the void.

The COVID-19 pandemic is distinct from prior epidemics in three ways:

1. **A global threat:** It is a pandemic, which means that the impacted community has come to encompass much of the world.
2. **Paucity of data:** It is a novel disease; health authorities are expected to educate and inform the public, though there is minimal verified information about the illness.
3. **Political accountability:** It is a geopolitical issue of significance for many countries, particularly China and the United States; governments are being called to account for their pandemic response by both their own citizens and other world powers.

The pandemic engendered a unique environment for the spread of misinformation and disinformation and reinforced the urgent need for better responses to counter such incidents. Sustained attention from a massive audience of affected people meant that a broad range of narratives—about the origin of the disease, for example, or about potential cures—spread globally as people shared them. Slow and unclear communication from health authorities revealed gaps in how authoritative information reaches people in crisis situations, both over social as well as broadcast media; when people are searching for answers and there is no reputable content to return, bad information may fill the void. Machinations by governments aiming to deflect blame for their handling of the disease, or to take advantage of the opportunity to weaken a geopolitical rival, reinforced the extent to which nation states can spread disinformation and propaganda across the full spectrum of communication technologies. State media broadcast properties, state-affiliated accounts on social platforms (such as diplomats, journalists, influencers), and covert bot and troll campaigns all helped propagate false or misleading information about the pandemic.

In summary: a combination of massive audiences seeking information, a scarcity of quality information to surface, institutional failures and politicization, geopolitical agendas, and determined activist and conspiracist communities leveraging the pandemic to push long-standing agendas to new audiences, created an environment in which researchers, journalists, fact-checkers, tech platforms, and civil society alike found themselves struggling to mitigate one misleading narrative after another.

To meet with any degree of success, all potential stakeholders—researchers, civil society organizations, journalists, social media tech companies, government, and other communicators who are responsible for connecting with the public—will have to collaborate on these solutions.

Without question, the COVID-19 pandemic brought many deep-rooted issues with the information ecosystem into stark relief. However, misinformation and disinformation narratives on myriad topics have become increasingly common over the past five years. Elections and political activities remain a focus of actors who execute deliberate disinformation campaigns. The stakes are high. Medical misinformation can significantly impact public health, and political disinformation can, at minimum, erode confidence in the legitimacy of democratic processes. Given the risks and the stakes, governments and targeted communities alike are searching for solutions to reduce the prevalence of malign and misleading narratives. To meet with any degree of success, all potential stakeholders—researchers, civil society organizations, journalists, social media tech companies, government, and other communicators who are responsible for connecting with the public—will have to collaborate on these solutions.

The issue of online disinformation reached mass public awareness with the Russian invasion of Ukraine and the discovery of Russian interference in the 2016 U.S. presidential election. At that time, cooperation between the various stakeholders was minimal. There was some collaboration among them, but efforts focused primarily on countering the threat of violent extremism, notably the readily attributable terrorist propaganda produced by ISIL. Health misinformation was still widely seen as an issue of free expression, and our understanding of the mechanics of online political influence operations was somewhat nascent. A small community of academic researchers were studying the people and organizations involved in these campaigns, but their work relied primarily on data from public Twitter conversations.

Access to data remains one of the overarching limitations on researchers' and policymakers' ability to understand and respond to influence operations, in terms of both proactive detection and forensic assessment. Efforts such as Social Science One and Facebook's recent decision to make its CrowdTangle analytics platform available to newsrooms and academic researchers have improved outside access, and yet much of the available data continues to provide insight primarily into engagement.[1] Engagement data can help researchers approximate how many people interacted with a particular piece of content or narrative, but it is not enough to answer important questions about what communities engaged with the content, whether a misinformation campaign changed the mind of a target, or whether or not a campaign increased polarization within a community or led people to believe or act on false information. That said, even though researchers might benefit from additional access, an offsetting factor is the significant privacy concerns associated with making certain types or quantities of user, community, or behavioral data available.

Multistakeholder cooperation offers a way forward. In an ideal scenario, we might envision a system in which a civil society organization or journalist flags content or accounts that seem anomalous. That anomalous content could be shared with a tech platform integrity team representative who has deep visibility into account activity on their platform. It could be shared with a quantitative social science researcher who has tools to assess how the content is being disseminated across platforms. If there are indications of foreign involvement, it might be shared with a relevant government actor who has additional insight into financial flows or other dynamics that might help unravel complex networks. Attribution of the operation would also be a collaborative effort. These far-reaching connections turn the process of detection and investigation into a multidisciplinary effort.

Such partnerships also may be useful from the standpoint of mitigating harmful effects of malign narratives. The tech platforms have visibility into affected communities. Civil society and fact-checking organizations trusted by those communities can spearhead the process of countering or correcting the narrative, or empathetically communicating to people that they have been misled. Governments might be involved in discussions about future deterrence if a foreign actor was implicated.

Efforts focused on mitigating the effects of misinformation and disinformation in the information ecosystem exist in some semi-organized capacities. Many others are informal and ad hoc.

Collaborative, jointly-owned efforts focused on mitigating the effects of misinformation and disinformation in the information ecosystem exist in some semi-organized capacities. Many others are informal and ad hoc. All those who are involved in these efforts should be working to remove barriers that prevent them from delivering their full potential value. In a 2019 whitepaper, *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, the Stanford Cyber Policy Center noted that one such initiative was the signing of the U.S. Cybersecurity Information Sharing Act (CISA) of 2015, which reduced legal barriers to sharing cybersecurity threat indicators.[2] The paper's authors offered a parallel suggestion that has yet to be implemented, but which democracies worldwide should consider as a means of significantly increasing access to data: legislatures should "establish a legal framework within which the metadata of disinformation actors can be shared in real-time between social media platforms, and removed disinformation content can be shared with academic researchers under reasonable privacy protections."[3] Additionally, to facilitate public-private information sharing, tech platforms should establish a coordinating body that enables the sharing of threat information between industry companies and can interface with appropriate government actors. One such model, used in dozens of other industries, is an ISAO (information sharing and analysis organization) or ISAC (information sharing and analysis center).[4]

Although early policy papers advocated collaboration and cooperation between actors focused on securing democratic elections, the COVID-19 pandemic has made it clear that misinformation and disinformation are broader in scope and global in impact. Influence operations are not going to cease; adversaries will not only continue to evolve but also continue to evade the legal, policy, and technical barriers put in place to stop them. Addressing this challenge necessitates a whole-of-society effort—it is time we worked to enable one.

Endnotes

1 "Social Science One," Institute for Quantitative Social Science, Harvard University, *https://socialscience.one/*; Naomi Shiffman, "CrowdTangle for Academics and Researchers," CrowdTangle, n.d., *https://help.crowdtangle.com/en/articles/4302208-crowdtangle-for-academics-and-researchers*.

2 Alex Stamos, Sergey Sanovich, Andrew Grotto, and Allison Berke, "Combatting State-Sponsored Disinformation Campaigns from State-aligned Actors," in Michael McFaul, ed., *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond* (Stanford, CA: Stanford Cyber Policy Center, 2019), 48–49, *https://fsi.stanford.edu/publication/securing-american-elections-prescriptions-enhancing-integrity-and-independence-2020-us*. For more on the affiliated event, see "Securing Our Cyber Future: Innovative Approaches to Digital Threats," Freeman Spogli Institute, Stanford University, 6 June 2019, *https://cyber.fsi.stanford.edu/securing-our-cyber-future*.

3 Stamos et al., "Combatting State-Sponsored Disinformation Campaigns from State-aligned Actors," 49.

4 Jaikumar Vijayan, "What is an ISAC or ISAO? How these cyber threat information sharing organizations improve security," CSO, 9 July 2019, *www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html*.