Carnegie Mellon University
Block Center for Technology and Society

Combating Disinformation One Month from the 2020 Election: **What Cities and States Can Do**

Introduction

In the past decade, disinformation campaigns on social media have gone from a tactic deployed by fringe groups to a comprehensive attack strategy used by state and non-state actors to undermine the legitimacy of United States elections, public health and other forms of American public life. For example, according to research from Oxford University, the number of countries targeted by organized disinformation campaigns doubled between 2017 and 2018. However, national governments are not the only target of disinformation campaigns. In recent months, we've seen numerous attacks targeting the ability of cities and states to respond to the pandemic and wildfires as well as undermining voting procedures.

With the 2020 election only a few weeks away, we all have a part to play to ensure U.S. elections at all levels of government are fair, transparent, and effective. Specifically, state and local public officials need to recognize that providing voters with accurate information on polling locations, voting procedures and other election processes is a critical part of their jobs. While fully combating disinformation at the state and local level will require legislative action, significant investments, and bureaucratic restructuring, there is much that elected officials and their administrations can do now. This brief is meant to provide specific action items for cities and states.

What disinformation looks like

There are three main sources of disinformation: Humans, bots, and cyborgs (a combination of humans and bots). Humans can be individuals acting alone, or those actors can represent an organization. Within the U.S., a significant amount of the disinformation shared by humans is rebroadcasted. According to researchers at Carnegie Mellon University, 77 percent of the disinformation spread by people in the U.S. related to the COVID-19 pandemic was rebroadcasted material from other individuals in the U.S. In addition to humans, a significant portion of disinformation is promoted by bots, computer algorithms programmed to spread information, or cyborgs, which are accounts that are run at times by humans and at times by bots. On Twitter, 42 percent of the top 50 most influential mentioners and 82 percent of the top 50 most influential retweeters related to the COVID-19 pandemic were bots.

Disinformation campaigns often leverage social media platforms' recommendation and marketing algorithms in order to target specific groups, including but not limited to women and underrepresented minorities. These campaigns may seek to drive individuals away from a platform, politicize otherwise apolitical issues, fuel hate speech and undermine democracy. In the case of COVID-19, disinformation campaigns have been organized with such goals as promoting conspiracy theories about the origin of the virus, politicizing the act of wearing a mask, and sowing unrest by pushing stories that democracy is an ineffective form of government during a pandemic. Experts worry that similar tactics and rhetoric are underway to delegitimize the 2020 election.

Me and the squad tryna catch the corona virus so we can skip work:

A COVID-19 disinformation meme satirically encourages viewers to intentionally catch the coronavirus.

There are many different forms of disinformation, and they often require a form-specific response. Frequently employed tactics of disinformation include videos, subconscious cues, deep fakes, and the mobilization of armies of bots and trolls. Memes *(pictured)* are also often employed to spread disinformation using pithy captioned images.

What mayors, governors and citizens can do now

In the coming weeks, there are specific things that are validated by research to be effective against election-related disinformation.

TIP	WHY IT MATTERS
Create a clear, proactive digital media/communications plan.	COVID-19 will make voting in the 2020 election different. Prepare ahead of time. Determine who will be responsible for day-of disinformation events (e.g., inaccurate voting locations, health concerns, etc.) and formulate a clear response strategy. The goal should be to have everything in place for a rapid response. Remember, disinformation campaigns often target the election process, not just candidates and their positions.
Use organizational accounts to deliver public messaging rather than individual politicians' accounts.	The politicization of topics is a major weapon of disinformation campaigns. By having a bureaucratic agency share information rather than a given individual or their social media team, you can be sure that the message appears politically neutral.
Strive to be accurate, consistent, timely and authoritative while spreading information.	Disinformation campaigns often aim to discredit government resources. By maintaining a reliable, professional and expedient online presence, you can outperform and outpace sources of disinformation.
Engage with local media.	Local media can be an important partner when providing the public with reliable voting information and combatting Election Day misinformation. Create points of contact and a strategy to quickly provide information and concerts to local media outlets.
Build a community of trust.	Engaging with local opinion leaders, key members of the community, local media and so on – and helping them to spread clear, accurate and timely messages – builds overall resilience of the community

Task digital media teams – or even volunteers – to check sources, verify the accuracy of election information from third parties and provide information back on a fact-checking site.	Communication teams, or even recruited volunteers, can help identify social media that is likely to be fake. Just as poll workers prepare to support voters on Election Day, digital teams can prepare to respond to real-time disinformation leading up to Election Day and let the public know what is true and what is not.
Before sharing a link, check the URL and be sure to consistently push and utilize official sites.	The domain name ending of a URL can tell you a lot about where information is coming from. For instance, a ".edu" domain ending indicates that a website is affiliated with an institution of learning. Watch out for clever workarounds, like ".com.co" which might appear legitimate at first glance.
If you see false information or information that you are not 100 percent sure about, don't share it.	Social media recommendation algorithms rely on engagement. Don't help propagate disinformation by driving traffic toward an unreliable source.
Don't underestimate satire.	As in the case of ingesting bleach to cure COVID-19, satire and humor can be a source of effective disinformation.
If you read a piece of disinformation on social media, call it out.	Sending posts that call out disinformation and state that another post is false will impact some readers.

While many of these tactics may seem intuitive or obvious, it is important to be vigilant about protecting the public from disinformation and maintaining a smooth flow of public messaging, particularly in times of crisis.

What cities and states can do for the long term

It is now well-documented that disinformation campaigns played an important and destructive role in the 2016 election. While we may not know for months or years the impact these actors and activities will have on the 2020 election, it's clear the problem is only getting worse. In the moderate and long term, cities and states will need fundamentally new tools to combat this new digital enemy. Doing so will require overcoming political, financial and bureaucratic hurdles.

Politically, there is often partisan disagreement on how to best address disinformation. Progressives often believe regulating social media platforms is the most effective route, while conservatives worry about impeding free speech. These differing views have made political and legislative action difficult.

In 2019, both Texas and California's state legislatures passed laws criminalizing deep fakes. Texas's S.B. 751 outlaws the publication and dissemination of deepfake videos intended to harm a candidate or influence election results within 30 days of an election, while California's A.B. 730 bans deep fakes aimed at harming a candidate's reputation "unless the campaign material contains a specified disclosure" within 60 days of an election. However, both bills make disinformation a domestic issue, doing little to combat foreign interference, and they have garnered criticism from First Amendment activists who are concerned that these laws may impede free speech. While the debate between the appropriate regulatory environment and individual freedom are legitimate, both sides should find consensus on the seriousness of disinformation and work together in areas less fraught with partisan disagreement. Public awareness and education campaigns are clearly in the public's interest, and should not be seen as Democratic or Republican solutions.

Financially, far too few resources are being invested to support and prepare municipal and state governments to combat disinformation. For example, disinformation that is patently lethal such as ingesting bleach to prevent or cure COVID-19, should be seen as a criminal issue rather than a partisan issue. A study by the University of Baltimore found that online fake news costs the global economy $78 billion each year, yet most cities and states have virtually no resources explicitly targeted to combating this. Federal resources, as well as technical and other support through partnerships with technology and social media companies, will be essential for states and municipalities to adequately defend against online threats.

State and municipal leaders will also need to redesign their own agencies to be better prepared to respond to local online attacks and false information. For example, research by Carnegie Mellon's Kathleen M. Carley found that 45 percent of all Twitter accounts discussing COVID-19 were likely bots. Yet this reality caught most departments of public health completely off guard as they traditionally do not have robust communication teams. Disinformation has completely redefined the demands of a modern communication and digital media strategy, and governors should respond with a new generation of communication teams.

Preparing the next generation of communications and digital media teams within the public sector

The days when interns ran a mayor's Twitter account are over. The onslaught of disinformation at the sub-national level calls for rethinking the role and obligations of municipal and state communication and digital media departments. For most state and local governments, social media platforms are maintained by communications and digital media teams as the primary goal historically was to communicate the office's political and policy agenda with the public. In the era of disinformation and misinformation, social media has taken on an entirely new meaning for elected officials. New models of operating that enable communications teams to identify and address disinformation are essential to ensuring elected officials continue to be authoritative, trusted sources of public information.

> **Today, state and municipal officials must see disinformation as a social cybersecurity threat and bring to bear the resources of their chief technology officers (CTOs) and cybersecurity teams in conjunction with communications and digital media.**

CMU's Kathleen M. Carley defines this new form of attack as "social cybersecurity," where political, social and technical acumen are needed to identify and successfully counteract it. Carley shows that the focus of most cybersecurity efforts is to stop the attacks aimed at impacting technology, such as stealing or destroying information, money or identities. But social cybersecurity is the use of technology to prevent the manipulation of individuals, groups or communities. To address these attacks, communications teams often lack necessary technical skills, while cybersecurity departments lack the statistical skills, communication acumen, and the political and social wisdom to identify political targets, "dog-whistles" and other linchpin commentary.

> **To address social cybersecurity in the age of disinformation, cities and states should construct inter-departmental teams between the Chief Technology Office and the communications and digital media teams. They should employ data scientists as part of digital media teams to support both assessment and communication.**

Beyond rethinking the role of the communications department, there are a number of things cities and states can do in the moderate- to long-term.

POLICY RECOMMENDATION	WHY IT MATTERS
Avoid blanket policies that "ban the bot."	Unilaterally banning bots could do more harm than good. Bots are useful for swiftly disseminating information during natural disasters and other time-sensitive emergencies.
Develop co-regulatory models with social media platform companies.	Working with industry to identify frameworks for how platforms should address different forms of election disinformation can be effective. For example, the European Commission's Code of Practice on Disinformation – an initiative between the Commission and companies like Facebook, Google and Twitter to deploy voluntary measures to tackle disinformation – was effective at addressing COVID-19 disinformation campaigns in Europe. Similarly, Governor Gavin Newsom created a partnership with social media companies that allowed California public health agencies to share public health information in the ad space on platforms such as Facebook.
Invest in media literacy strategies to create a more informed public.	Just as digital literacy has become a critical feature of most public education programs, media literacy needs to be incorporated into education programming for students and adults. There are currently dozens of online courses and tools that help citizens better identify and diffuse (or at least not spread) disinformation. States are well positioned to organize, promote and incorporate media literacy into existing digital literacy programming – both within the traditional K-12 education system as well as training centers such as public libraries.

Conclusion

From internet bullying to disinformation – while digital information sharing is by definition borderless – the impact of online activity plays out locally. And yet when we discuss the consequences and disinformation and the role of policy makers, local and state leaders are often neglected. But if properly resourced, informed and organized, municipal and state governments can be a community's first line of defense against online attacks. And as disinformation campaigns begin to target local issues and election processes, the role of local officials is only increasing. Gone are the days when issues of digital truth, transparency and accuracy are relevant to technology platform companies and national governments. Today, beginning with the 2020 election, everyone has a role to play in stopping disinformation.

More Resources

Daniel Castro. "Deepfakes Are on the Rise — How Should Government Respond?"
Government Technology, 2020.

"Countering Mis- And Disinformation Amid COVID-19," National Governors Association, 2020.

"Disinformation and Elections: How Election Officials Can Respond," Cybersecurity and Infrastructure Security Agency.

Karen Hao. "Nearly half of Twitter accounts pushing to reopen America may be bots,"
MIT Technology Review, 2020.

"Integrating Social and Behavioral Sciences (SBS) Research to Enhance Security in Cyberspace,"
National Academies Press, 2019.

Daniel Tkacik. "Q&A with Kathleen Carley on the spread of coronavirus disinformation," *Tech Xplore*, 2020.

Darrell M. West. "How to combat fake news and disinformation." Brookings, 2017.

About the Block Center for Technology and Society at Carnegie Mellon University

Addressing technological disruption from the perspective of economics, organizations and public policy, the Block Center's projects seek to ensure that the benefits of technological change are widely shared, opening new paths to prosperity for all. Learn more about the Block Center for Technology and Society

About the Center for Informed Democracy and Social-cybersecurity (IDeaS) at Carnegie Mellon University

The Center for IDeaS at CMU was launched in 2019 with generous support from the John S. and James L. Knight Foundation to study how disinformation is spread through online channels and address how to counter its effects to preserve and build an informed citizenry. The Center is co-directed by CMU professors Kathleen M. Carley in Carnegie Mellon University's School of Computer Science, Institute for Software Research, and David Danks in Dietrich College of Humanities and Social Sciences, Philosophy Department. The Center takes a multidisciplinary approach, engaging researchers from across the university to examine and develop responses to technological and human facets of issues. Learn more about IDeaS