Disinformation in Democracies: Strengthening Digital Resilience in Latin America
The Adrienne Arsht Latin America Center broadens understanding of regional transformations through high-impact work that shapes the conversation among policymakers, the business community, and civil society. The Center focuses on Latin America’s strategic role in a global context with a priority on pressing political, economic, and social issues that will define the trajectory of the region now and in the years ahead. Select lines of programming include: Venezuela’s crisis; Mexico-US and global ties; China in Latin America; Colombia’s future; a changing Brazil; Central America’s trajectory; combatting disinformation; shifting trade patterns; and leveraging energy resources. Jason Marczak serves as Center Director.

The Atlantic Council’s Digital Forensic Research Lab (DFRLab) is at the forefront of open-source reporting and tracking events related to security, democracy, technology, and where each intersect as they occur. A new model of expertise adapted for impact and real-world results, coupled with efforts to build a global community of #DigitalSherlocks and teach public skills to identify and expose attempts to pollute the information space, DFRLab has operationalized the study of disinformation to forge digital resilience as humans are more connected than at any point in history.

For more information, please visit www.AtlanticCouncil.org.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report’s conclusions.

© 2019 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005


March 2019
Disinformation in Democracies:

Strengthening Digital Resilience in Latin America

This report is a collaborative effort between the Digital Forensic Research Lab (DFRLab) and the Adrienne Arsht Latin America Center of the Atlantic Council.

By: Luiza Bandeira, Donara Barojan, Roberta Braga, Jose Luis Peñarredonda, Maria Fernanda Pérez Argüello
Foreword

As the sun rose on 2019, democracies across Latin America awoke to new leaders and new administrations looking to fulfill promises of change. In Brazil, the new year marked Jair Bolsonaro’s inauguration, and in Mexico and Colombia, Andrés Manuel López Obrador and Iván Duque, respectively, continued to implement their nascent government agendas.

Having recently led the Organization of American States (OAS) observation missions of some of these elections and as these country agendas were taking shape, I laid out my own vision for what democracy holds in the short and long terms—particularly the digital dangers that are likely to affect political contests and their legitimacy.

Digital technologies have immense potential to improve lives. But, as the 2018 elections in Latin America showed, they can also be used to exacerbate the spread of disinformation and misinformation in ways that can impact political decision-making and electoral outcomes.

In 2018, the Atlantic Council’s Digital Forensic Research Lab (DFRLab) and Adrienne Arsht Latin America Center partnered to strengthen digital resilience in elections by identifying, exposing, and explaining instances of disinformation, working alongside Latin American media, civil society, and academic organizations. The effort, #ElectionWatch Latin America, was—and continues to be—a necessary step in addressing the spread of disinformation and misinformation facilitated by the rapid permeation of online technologies.

Governments, technology and social media companies, civil society, and media don’t yet fully understand the challenges disinformation poses to democracy. These stakeholders, each with different sets of motivations, do not yet fully see eye to eye on the best way to address the rise of influence operations online. Meanwhile, regulatory frameworks remain outdated as technologies evolve at a faster pace than the laws that regulate online abuses and punish bad actors.

How can society protect freedom of expression while simultaneously combatting disinformation in the digital realm? And how can public and private-sector stakeholders work alongside media and others to effectively manage or contain threats brought on by disinformation and misinformation?

This report seeks to contribute to ongoing discussions with proposals for how to address these growing challenges. These conversations must be had in Latin America, but the implications and lessons extend far beyond the region. Now more than ever, comprehensive solutions are needed to mitigate the negative impact of disinformation while promoting the many benefits of direct citizen engagement.

This year, more than eighty elections are taking place worldwide. Many will decide leaders of key democracies—in Latin America, Europe, Asia, and beyond. Failing to create deeper understanding, and to better align efforts to address the spread of false information around elections, could significantly undermine public trust in the democratic process for decades. But, getting it right will bring immense society-wide benefits.

Laura Chinchilla
Chair, Kofi Annan Foundation; Former President of Costa Rica; Member, Adrienne Arsht Latin America Center Advisory Council, Atlantic Council
# Table of Contents

EXECUTIVE SUMMARY ................................................. 3

INTRODUCTION ......................................................... 4

DISINFORMATION IN THE 2018 ELECTIONS

   BRAZIL ................................................................. 6

   MEXICO ............................................................... 20

   COLOMBIA .......................................................... 30

RECOMMENDATIONS .................................................. 42

CONCLUSION ........................................................... 46

ACKNOWLEDGMENTS ................................................... 47

GLOSSARY OF KEY TERMS ............................................. 48

ABOUT THE AUTHORS ............................................... 50

ENDNOTES ............................................................... 52
Between May and October 2018, three of Latin America’s largest democracies—Brazil, Mexico, and Colombia—elected new heads of state, congress members, and local officials in a series of polarized, contentious elections. In a region in which the number of cell phones often exceeds the number of voters in many countries, political debates dominated the online space and the world of messaging platforms—disinformation and misinformation followed, intricately intertwined into those conversations.

A rapidly evolving information environment—wherein innovation often outpaces traditional security measures and governance at the private and public levels—became a catalyst and a vector for the spread of rumors and false information. Disinformation actors, whether through organic disinformation or by employing artificial amplification, provoked fear and anxiety, and sought to illicitly influence voters, undermining the electoral process along the way.

To address this complex set of challenges, the Atlantic Council’s Adrienne Arsht Latin America Center and its Digital Forensic Research Lab (DFRLab) partnered with local organizations to identify, expose, and explain disinformation, to promote increased dialogue, to support concerted action, and to increase digital and media literacy as a bulwark of democracy. #ElectionWatch Latin America—as the effort was called—shed new light on the ways disinformation, misinformation, and automation appeared within the context of each country’s election environments and influenced outcomes.

In Brazil, Atlantic Council research conducted in real time found that disinformation comprised primarily organic disinformation—driven by polarization and a lack of trust in institutions. In Colombia, the Atlantic Council observed a similar trend, exacerbated at times by political leaders and the media’s purposeful or accidental spread of false information. In Mexico, the Council found automation and artificial amplification to be more prominent. Atlantic Council researchers uncovered actors who hired commercial bots for financial gain and used political bots for the spread of specific electoral messages. At the state level, meanwhile, disinformation about the electoral process exacerbated polarization.

In response to the challenges posed by disinformation, stakeholders mobilized to strengthen digital resilience. Impressive, multi-stakeholder engagement from electoral bodies, international institutions, technology and social media companies, civil-society and academic organizations, and the media comprised a series of nascent, growing, and evolving efforts. Lessons learned from 2018 will fuel solutions to the global challenge of disinformation for decades to come. By highlighting some such lessons and laying out potential solutions to be considered in the next phase of this fight, the Atlantic Council today lays out a vision for a future where facts and truth prevail.

Authentic communications underpin the legitimacy and resilience of democracies around the world. Through a multi-stakeholder approach, society must continue to understand disinformation, to strengthen digital resilience, and to transform the digital engagement space, not only ahead of future elections in Latin America, but ahead of elections in every corner of the globe.
The world is more connected than ever, with more than four billion people engaged online, and 3.5 billion on social media. In Latin America, where many countries are mobile first, online connectivity is widespread and escalating. In 2019, more than 101 million mobile-phone users in Brazil will access the Internet from their devices, up from around 72 million in 2015.1

It is no surprise, therefore, that new challenges have emerged over the years in conjunction with the changing tides of information consumption and connectivity. Disinformation (false information spread with an intent to deceive) and misinformation (false information spread without intent) have begun to deeply influence communications. Today, critical consumption of information, with an eye for disinformation and misinformation, can be the difference between a grandfather in Brazil being lauded or denigrated for making putty on YouTube. Unstopped, false rumors can lead to the mob lynching of a young Indian man wrongfully accused of kidnapping children in his village.

That moment when a person makes the decision, from the comfort of his or her couch, to send a seemingly real video about electronic voting fraud to followers and networks on WhatsApp, Twitter, or Facebook, may very well risk incremental and lasting damage to the democratic ideals and institutions underpinning freedoms and rights in their country.

More than in any Latin American electoral cycle to date, disinformation and misinformation made their rounds on social media in Brazil, Mexico, and Colombia in 2018. False narratives, hyperpartisan blog posts, edited images, and misleading videos fueled
increased polarization as voters headed to the polls.

Society raced to understand how and why disinformation spread in the Western Hemisphere. Some blamed technology companies and social media companies. Others blamed the political “establishment.” Yet others blamed the traditional news media. Meanwhile, a spotlight turned on WhatsApp as the messaging platform dominated headlines in Brazil. And, in the United States, Congress called hearings to determine the feasibility and risk associated with potential Russian interference in Mexico’s elections.

While it may be tempting to blame a few organizations or platforms for the challenges associated with disinformation and misinformation, instances of such during the 2018 elections in Latin America were a byproduct of a confluence of factors. Economic downturns, unemployment, corruption, mistrust in politicians, and a desire for change came together to create an environment ripe for the spread of falsehoods online. Illicit actors, networks, and social media users bought and sold likes and shares on social media, and journalists throughout the region struggled to get ahead of disinformation, while simultaneously working to prevent the amplification of false news.

In Brazil, as the country descended into an economic recession and grappled with a wave of corruption that implicated nearly two thirds of politicians in the lead up to the presidential elections, organic disinformation spread like wildfire—at times, with politicians exacerbating disinformation and misinformation narratives.

In Mexico, Atlantic Council researchers and partners detected automation in national and local politics. Moguls like Carlos Merlo thrived on a diseconomy of disinformation, monetizing the buying and selling of likes and shares on social media, and journalists throughout the region struggled to get ahead of disinformation, while simultaneously working to prevent the amplification of false news.

In Colombia, only a short time after the referendum on the proposed peace agreement between the government and the Revolutionary Armed Forces of Colombia (FARC), a polarized race gave way to blame games between the right and the left, with each side using disinformation to attack the other. Media, in their attempt to combat it, often unintentionally amplified disinformation.

At the core of the Atlantic Council’s mission is the belief that democracy relies on debate. In any democracy, facts are fundamental to that productive debate. Unfortunately, the massive consumption of unbalanced or intentionally misleading information online has the potential to throw democracy off balance.

This is why, in 2018, the Atlantic Council’s Adrienne Arsht Latin America Center and its Digital Forensic Research Lab partnered to create #ElectionWatch Latin America to identify, expose, and explain disinformation where and when it happened around elections in Brazil, Colombia, and Mexico.

Going beyond fact-checking and working alongside partners in the region—including think tanks, media, and universities—and in conversation with technology firms and electoral authorities, the Atlantic Council’s #ElectionWatch Latin America researchers used open-source data (anything publicly available online) to explain how cases of disinformation emerged, who was affected, who amplified stories, how they spread, and what came out of that circulation.

Rather than assuming its own credibility, through #ElectionWatch Latin America the Atlantic Council harnessed open-source information to explain disinformation with an element of transparency; the findings and the tools used to conduct these investigations were available for anyone to verify. In parallel, the council undertook capacity-building trainings that leveraged on-the-ground knowledge, and built a robust and sustainable community of local nongovernmental actors in the information space.

The findings of this year-long effort are highlighted in this report. But the #ElectionWatch Latin America effort is part of a broad, concerted effort to strengthen digital resilience in Latin America and beyond. The challenges have not dissipated post-elections, and more must be done to strengthen a field ready to tackle changing communication trends. The Atlantic Council, in conversations with partners on the ground, takes a first step to outline suggested recommendations to protect public debates from those who would seek to undermine them in the digital-engagement space.

Digital resilience is not an issue to be approached by one or two organizations. Truly global challenges by their very nature, disinformation and misinformation must be addressed through the collective efforts of governments, technology companies, telecommunications organizations, civil society, media, and academia.

As the world dives ever more deeply into the sea of online engagement, now is the time to ensure that democratic ideals and freedoms are upheld, while taking action to prevent illicit online activity. Any sustainable solution to the problem of disinformation and misinformation will need to come from honest conversations among diverse actors, including in the private and public sectors, media, and civil society. This report seeks to support these actors, to strengthen a truly multi-stakeholder approach. The time for digital resilience is now.
**KEY FINDINGS**

| Disinformation in Brazil’s elections included organic disinformation spread through encrypted messaging platforms. | Hyperpolarization and a lack of trust in institutions—spanning government, media, and civil-society organizations—created an atmosphere in which disinformation spread quickly, with compounding effects. | Countering disinformation narratives, rather than instances of disinformation, may be more impactful in assuring that disinformation does not set the agenda for electoral debates and media coverage. |

**CONTEXT**

On October 28, 2018, Brazilians elected former Army Captain Jair Bolsonaro as their next president, following a polarizing and contentious race. Far from ordinary, the 2018 general election took place at a unique point in Brazilian history, one that followed a deep economic recession and a political crisis that saw scores of politicians jailed or investigated for corruption. The economic and political crises accentuated violence and insecurity—in 2018, petty crime soared, and homicide rates hit a record high of thirty per one hundred thousand people. Taken together, these factors fostered widespread rejection of the established political parties—especially the Workers’ Party (Partido dos Trabalhadores, or PT), which had governed Brazil for most of the previous fifteen years. They also helped elevate change candidate Jair Bolsonaro, a legislator previously on the sidelines of Brazil’s political scene, known mainly for his controversial statements during nearly thirty years in Congress. Bolsonaro was elected with 55 percent of the vote in the runoff election—a victory attributed not only to the complicated economic and political moment in which Brazil found itself, but also to his effective use of social media as a primary means of connecting with Brazilian voters.
Economic Stagnation and Brazil’s Operation Car Wash

To understand how Brazil’s economic stagnation (marked by a shrinking of the economy and peak unemployment), political mistrust (fostered by the Lava Jato or Operation Car Wash corruption investigation), and insecurity (exacerbated by rising crime rates) intertwined with deep distrust in a hyperconnected, mobile-first society to shape debates and the spread of disinformation around Brazil’s election, it is important to consider sentiments in Brazilian society leading up to the 2018 elections.

Between 2013 and 2018, debates in Latin America’s largest democracy became increasingly polarized. Mass street protests in 2013 sparked ever-widening divisions during and after the 2014 presidential race that saw President Dilma Rousseff narrowly reelected. As Brazil became engulfed in political and economic crises over the next five years, divides became starker. The crises, mutually reinforced by and intertwined with Operation Car Wash, significantly affected the PT. The impeachment of President Dilma Rousseff of the PT party during her second term in 2016, the arrest of former President Luiz Inácio Lula da Silva (the most visible face of the party and his subsequent barring from the 2018 election), and the party’s perceived inefficiency in addressing Brazil’s crises over its years in power, led to notable rejection of the “left” and the PT in the 2018 presidential election.

Jair Bolsonaro faced off in a contentious race against Fernando Haddad, who took over as the PT candidate after Lula was barred from running. Though Lula led in polls before being removed from the race, Bolsonaro took the lead against Haddad. Bolsonaro presented himself as an outsider and ran on a platform that proposed liberal economic policies and conservative values as a way of undoing the progressive policies implemented by the Lula and Rousseff administrations. He also advocated a strong security platform that included easier access to guns for Brazilians.

Lack of Institutional Trust

Despite having little financing or television and radio air time—two components that had largely determined presidential victors in the past—Bolsonaro effectively used social media as his primary means of connecting with Brazilian voters already deeply distrustful of politics as usual. In 2018, Brazilians’ trust in institutions reached its lowest level.
Almost 90 percent of Brazilians watch television to stay informed, and television is the most important outlet for 63 percent of Brazilians—four broadcasters (Globo, SBT, Record, and Band), dominate the Brazilian broadcast market, capturing more than 70 percent of the Brazilian audience per 2017 numbers.12

While Internet use is on the rise and television consumption rates remain high, print newspapers are losing ground.13 Only 3 percent of Brazilians use newspapers as their main medium for staying informed, and 12 percent say they use newspapers along with other media. Between 2014 and 2017, the circulation of the eleven most widely sold print newspapers fell by 41 percent, to 736,346—the number of digital subscriptions has increased marginally, but does not compensate for the losses in print circulation.14 As a result, since 2017, Brazilian newspapers have tightened their paywall policies.

In Brazil’s information space—as, increasingly, in other countries throughout the world—it is important to note there is now a gap between where news is now published and where information is consumed. With newspaper consumption in decline, readers increasingly use messaging platforms like WhatsApp to access information. Despite this trend, professional journalism still does not extensively publish news on the platform, as they have not yet found a sustainable business model for use of the application.

### TABLE 1

<table>
<thead>
<tr>
<th>Medium</th>
<th>1st option</th>
<th>2nd option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Television</td>
<td>63</td>
<td>89</td>
</tr>
<tr>
<td>Internet</td>
<td>26</td>
<td>49</td>
</tr>
<tr>
<td>Radio</td>
<td>7</td>
<td>30</td>
</tr>
<tr>
<td>Newspapers</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Magazines</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Outdoor advertisements (billboard, bus, elevator, metro, airport)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Doesn’t know/didn’t reply</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Brazil’s Election Ecosystem

Voting in Brazil is mandatory for literate citizens between the ages of 18 and 70; in 2018, 147 million people were registered to vote in the country. Presidential elections take place every four years. Presidents are elected by the majority of voters in a two-round system, with the possibility for reelection to a second term. Along with presidential elections, the country votes for members of Congress and state governors every four years.

Brazil is a multiparty system; in the 2018 general election, the country had thirty-five registered parties. Parties receive public funding for elections and, since 2015, corporate donations have been banned. Notably, Brazil has relied on an electronic voting system for more than twenty years, since 1996.

Elections at the municipal, state, and federal levels in Brazil are organized and monitored by the Justiça Eleitoral (Electoral Justice). The most important electoral authority is the Tribunal Superior Eleitoral (the Superior Electoral Court or TSE), and each state has its own state court. The Electoral Justice is responsible for including voters in the voter’s registry, monitoring parties’ fundraising and expenditures, and verifying who can run for office. The TSE determines how much free campaign time on television and radio each party will have, based on its representation in the Chamber of Deputies, the lower house of Congress.

The Electoral Justice handles the logistics of elections, including choosing polling places, training personnel and distributing electronic voting machines throughout the country. The Electoral Justice also deals with electoral lawsuits, such as electoral crime and inspection of campaign advertising.

The activities of the Electoral Justice are monitored by the Ministério Público Eleitoral (the Electoral Public Ministry, also known as the Electoral Public Prosecutor’s Office), which can initiate legal action in cases concerning parties and candidates, in addition to monitoring the legality of voting at polling stations. The Electoral Public Ministry oversees the legitimacy of various components of the electoral process, including voter registration, party conventions, registration of candidacies, campaigns, and electoral propaganda. Both federal and state law enforcement investigate, and act to prevent, electoral crimes.

Disinformation and Misinformation in the 2018 Elections

To inform, expose, and explain disinformation and misinformation ahead of and during the electoral cycle in Brazil, the Atlantic Council partnered with leading think tank and higher education institution Fundação Getulio Vargas’ Department of Public Policy Analyses (FGV DAPP)—whose Digital Democracy Room reinforced strengthening of digital resilience in Brazil—and leading news outlet Jornal O Globo. As part of #ElectionWatch Latin America in Brazil, the Atlantic Council conducted research over the span of three months—from August to October 2018—and published on an ongoing basis. Atlantic Council findings showed fringe partisan websites emerging and contributing to hyperpartisan debates, organic disinformation spreading at high rates, and the role of WhatsApp as a vector for disinformation.

The Increased Relevance of Partisan Media Versus Traditional Media

As polarization grew in Brazil, so too did hyperpartisan websites. In the past, these websites have been called “fake news” websites. However, this designation does not accurately describe these websites, which combined “decontextualized truths, repeated falsehoods, and leaps of logic to create a fundamentally misleading view of the world,” rather than publishing completely fabricated stories—as was the case in the US election of 2016.

By adopting sensationalist headlines and appealing to emotions, these websites became increasingly popular. Atlantic Council investigations conducted as part of #ElectionWatch research in Brazil found, for example, that partisan websites outperformed traditional independent media in the corruption debate in the six months that preceded the electoral campaign.

At least one hyperpartisan website benefited from inauthentic amplification to spread its messages. The website República de Curitiba (Republic of Curitiba, a reference to the city where the Lava Jato corruption investigation had its headquarters), a pro-Bolsonaro blog, was the site with the second highest rate of engagements during the elections. In December, Facebook took down the República de Curitiba page due to inauthentic coordinated behavior—online behavior intended to deceive audiences about its authors or motives, conducted by several users in coordination with one another (see table 2). This inauthentic behavior is banned on Facebook.

While hyperpartisan websites flourished, independent media outlets were accused of publishing “fake news” during the elections. This criticism was led by then-candidate Bolsonaro himself, a vocal critic of...
One week before the first round of voting, protests against Bolsonaro took place. Posts by Bolsonaro supporters and pro-Bolsonaro pages on Twitter and Facebook claimed the media were artificially inflating the number of protesters at the rallies. Some users and pages shared edited images and pushed narratives suggesting the same images were being shared by the news media. These users and pages also disseminated the idea that the Jornal O Globo newspaper had published a picture of a different manifestation claiming it was from the anti-Bolsonaro rally. However, the picture was authentic, as Atlantic Council #ElectionWatch research showed.

Independent media were also accused of manipulation in one of the most significant cases of electoral violence registered during the election period. Capoeira Master Moa do Katende was murdered on October 7, 2018, on the night of the first round of elections. The suspect, a Bolsonaro supporter, was arrested and, according to law enforcement, confessed his political motivation for the crime—the victim supported PT candidate Fernando Haddad. However, while in front of television cameras, the suspect denied this political motivation. Per Atlantic Council findings, some independent news outlets failed to effectively relay his version of the story and were accused of publishing “fake news” by partisan websites that claimed the murder was not politically motivated. These partisan websites, however, ignored the police’s version of events, failing to tell the entire story.

Coordinated Organic Digital Engagement Prompted by Political Divisions

As disinformation and misinformation emerged, researchers found it difficult to establish original authorship and to quantify how organized the spread was during the elections. The Atlantic Council used open-source methodologies to establish who were the main amplifiers of these messages on open social media platforms such as Facebook and Twitter. Atlantic Council research found that the electoral race in Brazil was marked primarily by organic online engagement. Disinformation and misinformation generally garnered traction after being shared by “influencers” whose messages were then further disseminated by their followers.

Flávio Bolsonaro, Jair Bolsonaro’s son, and Joice Hasselmann, a former journalist and congresswoman, were two influencers that took part in the spread of videos wrongly suggesting fraud in electronic voting machines, per a Tribunal Regional Eleitoral of the state of Minas Gerais investigation in the case of the former and a Tribunal Superior Eleitoral conclusion in the case of the latter. And, after Jair Bolsonaro was stabbed, both his followers and his opponents spread false news.
information on Facebook groups and pages—while the left claimed Bolsonaro had staged that attack, the right claimed the attacker was a member of the Workers’ Party. Both claims were false.\(^{30,31}\)

These messages were then shared by the influencers’ followers. Bolsonaro’s supporters, in particular, were very active on social media.\(^{32}\) They often acted in coordination, though not necessarily using automation or artificial amplification by bots or botnets. This became evident, for instance, during the migration of Bolsonaro supporters to the alt-right social media platform Gab.ai. The most retweeted post read “Let’s up the hashtag #MeSeguoenGab (follow me on Gab).” The hashtag had twenty-five thousand mentions, and no indication of automated amplification was found.\(^{33}\)

#ElectionWatch Latin America research also detected campaigns on Facebook, Twitter, and WhatsApp prompting users to boycott the media and to “dislike” videos on YouTube.\(^{34}\)

Bolsonaro himself was very active on social media. On Facebook, for instance, none of the 12 other candidates who ran for the presidency came close to his audience engagement and reach. Bolsonaro finished the race with 8.6 million “likes” on his official Facebook page—runner-up Fernando Haddad garnered 1.8 million (see table 3).

**WhatsApp as a Vector for Disinformation**

The messaging application (app) WhatsApp was a vector for disinformation in the 2018 Brazilian elections. While discussions about disinformation in Brazil focused on WhatsApp and its potential influence on voters’ choices, because the app is encrypted and has no public API, there are no comprehensive metrics available to verify the extent to which disinformation or misinformation was shared within the platform. Per WhatsApp, the platform also does not have a search function and is not built for users to garner large followings. Per 2017 estimates, the application is used by at least 120 million people in Brazil—according to 2019 data from the company, WhatsApp has more than 1.5 billion users worldwide. The app utilizes end-to-end encryption, enabling only the sender and receiver of a message to access its content—the mechanism is aimed at preserving privacy and security.\(^{35}\) The popularity of the app in Brazil and in other countries, nonetheless, is partly attributed to economic reasons, rather than only to privacy concerns—telecommunications companies, in partnership with Facebook, adopt “zero-rating” policies that allow users to access the platform without tapping into their mobile data plans.\(^{36,37}\) This is also sometimes the case for other social media companies. Being a messaging platform rather than a broadcast...
social media platform, WhatsApp has no timeline or newsfeed comparable to those on Facebook and Twitter. Each piece of content a user receives on WhatsApp is sent directly to them or to a group of which they are a part. This means the app is perceived as a private environment to communicate with friends and family.

Nevertheless, the app also has broadcast features that allow for broader communication and that at times enable messages to go viral. By the first round of elections on October 7, 2018, each user could create up to 9,999 groups, each with up to 256 people, or single lists that broadcasted a message to 256 contacts at the same time. Users could also forward a message to up to twenty contacts simultaneously. Shortly before the campaign kicked off in August 2018, WhatsApp added a label that identified forwarded messages; prior to that, users had no way of knowing whether the author of a message was the person who sent it or if this person had forwarded the text from one of their contacts. In December 2018, WhatsApp restricted forwarding from twenty to five contacts.

The widespread use of WhatsApp and its perceived privacy—because groups and forwarding features sometimes result in users not realizing a message sent could be circulated widely within other networks on WhatsApp—combined with encryption and zero-rating policies, represents a triple challenge in the information environment.

First, in Brazil’s information space, as noted in the previous section, there is a gap between where news is published and where information is consumed. Readers increasingly use WhatsApp to access information, but professional news outlets do not publish news on the platform in any consistent way. Since there is no effective means of tracking how a piece of information is shared nor to obtain metrics to comprehensively verify audience engagement, it is difficult to find a sustainable business model for news on WhatsApp. This means journalists end up using traditional channels (their websites and social media) to publish news, while readers flock to a different channel (WhatsApp) to get informed, resulting in a gap between producers of trustworthy news and readers. This gap can be exploited.

Second, because access to websites outside zero-rating data costs money, there is a disincentive to share more informative links (like news articles) and an incentive to share less informative content (like images and memes). Additionally, many people avoid clicking on links that would take them out of WhatsApp to verify messages, especially since these messages are often sent by friends and family who are considered trustworthy sources. This reduces the likelihood that readers will use external sources to verify information they receive on WhatsApp.

Finally, it is difficult to track the spread of a message on WhatsApp at the scale or speed at which content circulates. Currently, because of the way WhatsApp is designed, the messaging platform does not allow for automatic notifications to readers alerting them that the information they are sharing is false, for tracking the performance of articles debunking false news, for the mapping of how narratives are amplified, or for complete removal of content with false information from the app. Importantly, because of encryption, it is difficult for researchers to use WhatsApp data to identify who the first person was to post a message containing false or misleading information.

Thus, researchers and journalists in Brazil focused on WhatsApp messages shared by consumers with fact-checkers and on “public” or “open” groups—groups of up to 256 people that could be accessed through links shared on the Internet, usually on Facebook. Of the public groups analyzed by researchers, many were connected to Bolsonaro.
supporters, with his own family being part of some.

While WhatsApp did not disclose the exact number of public groups that exist, the company indicated that worldwide approximately 10 percent of messages are sent in groups comprising up to 256 people. According to the company, most groups have fewer than ten people. During the election cycle, WhatsApp public groups often functioned like messaging pyramid schemes. Group members received material that they disseminate to their personal networks, who shared it with other networks, rippling distribution and amplification to a much larger audience.

While it was not possible to access complete data about the spread of disinformation within the encrypted platform, by tracing the most-shared messages on public groups, researchers and fact-checkers were able to show that those widely shared were either false or taken out of context. Moreover, a study by Brazil’s Instituto de Tecnologia e Sociedade, or ITS Rio, found users spreading a high number of messages in short intervals, as well as profiles with no names and impersonal profile pictures, suggesting automation was used in these public groups.

In addition to the public groups, media reported spam being shared with thousands of WhatsApp users. Though it is still unclear whether these messages contained disinformation, this has prompted discussions about the possibility of the app being used to circumvent campaign finance laws.

Narratives

ElectionWatch research in Brazil showed the main narratives circulating on WhatsApp were most often not different from those disseminated on Facebook or Twitter. This means WhatsApp is not necessarily the beginning or the end of false information. Rather, it works as a part of the information ecosystem, in which disinformation spreads. It also implies that debunking narratives, rather than debunking individual messages, might be more fruitful to preventing the spread of disinformation and misinformation.

<table>
<thead>
<tr>
<th>Narrative</th>
<th>Background</th>
<th>Examples of False Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electoral fraud</td>
<td>Independent analyses of Brazil’s electronic voting system found vulnerabilities that make the system susceptible to a potential hack. In twenty years, no consistent evidence of fraud has emerged.</td>
<td>Videos on WhatsApp showed voting machines allegedly forcing voters to cast a ballot for Fernando Haddad, the Worker’s Party candidate.</td>
</tr>
<tr>
<td>Child sexualization and “gender ideology”</td>
<td>In 2011, a government program on public health aimed at promoting acceptance and preventing homophobia in schools was cancelled after conservatives denounced it as a “gay kit” intended to sexualize children.</td>
<td>Candidate Fernando Haddad, who was the minister of education when the project was discussed, was accused on WhatsApp of being a pedophile and a supporter of incest. Messages also claimed that, if he were elected, children would become the property of the state at the age of five and their gender would be chosen then.</td>
</tr>
<tr>
<td>Anti-left and anti-Workers’ Party messages</td>
<td>The left-wing PT governed Brazil for thirteen years and saw many of its politicians accused of corruption. The country was also engulfed by an economic crisis toward the end of the PT’s mandate.</td>
<td>Images were circulated of a check that was supposedly part of a PT corruption scheme. Messages alleging the PT was communist and Brazil would become the next Venezuela were also shared widely.</td>
</tr>
<tr>
<td>Anti-media content</td>
<td>Traditional media faces a crisis of trust. Bolsonaro continues to be a vocal critic of the media and often claims they publish “fake news.”</td>
<td>Messages claimed articles published by the media were wrong. Campaigns called for the boycott of media outlets.</td>
</tr>
</tbody>
</table>
Although it is not possible to determine who spread these messages at scale—because of the encrypted nature of WhatsApp and due to the pyramid-scheme design of groups—then-candidate Jair Bolsonaro was one, if not the main, beneficiary of these narratives. Research has shown that the “gay kit” and the “electoral-fraud” stories, which clearly targeted Haddad and bolstered Bolsonaro’s campaign messages, were the most shared messages on Twitter, Facebook, and YouTube. However, the then-candidate was also the victim of rumors, most connected to his stabbing, which left-wing groups claimed had been staged to garner popular support.

### IMPACT ON THE ELECTIONS

The direct influence of disinformation on voter preferences in the Brazilian elections is difficult to quantify. Two opinion polls conducted in October showed different results. After the first round, an Ibope poll suggested three in four voters did not receive negative messages about any candidates on WhatsApp the week prior to voting. Hence, per Ibope, the impact of WhatsApp was limited. Another poll, by Idea Institute, suggested that 98 percent of Bolsonaro voters were exposed to false messages and 90 percent believed them. Opinion polls also might be affected by misreporting.

Although it is not possible to affirm with certainty how disinformation and misinformation affected votes, both did cause unrest at the national level during the election cycle. The most visible example was the spread of the electoral fraud narrative, which was worrisome because it further eroded trust in institutions. Per Atlantic Council #ElectionWatch Latin America reporting, suspicions about electoral fraud gained momentum when Bolsonaro published a video on his Facebook page claiming the possibility of fraud was concrete. This happened around the same time polls indicated Bolsonaro was losing support ahead of the first round of voting on October 7.

The day of the first round of voting was marked by claims of electoral fraud, many false. One of the more widely shared videos showed a voting machine allegedly forcing voters to cast a ballot for Haddad, the Worker’s Party candidate. This video was shared by one of Jair Bolsonaro’s sons on Twitter and quickly gained traction, despite statements made by Brazil’s electoral court affirming the video had been manipulated. At polling stations across Brazil, voters claimed voting machines were not working and registered formal complaints with the Electoral Justice. Some claims were dismissed by the police. The Federal Police and the Electoral Justice, however, did not publish a full report with the outcomes of all investigations, making it difficult to examine the scale of the problem and the extent to which the problems involved any kind of fraud.

Similar claims of electoral fraud circulated around the second round of voting. One person was arrested in the state of Rondonia after publishing a video telling people to use glue to break voting machines to stop people...
from voting for the PT.\textsuperscript{61} The president of Brazil’s top electoral court also received online threats.\textsuperscript{62}

Disinformation also impacted Brazil’s election by setting the agenda for media coverage and political debates online. Candidates and news outlets spent countless hours responding to rumors and false news and, in the process, spent less time covering the platforms being proposed by the candidates, and their history and achievements as politicians.\textsuperscript{61} For example, during the campaign period (August 15 to October 28), the term “fake news” was mentioned 1.9 million times on Twitter. The numbers illustrate how disinformation and false narratives became something to which candidates, media, and the voters had to react.

Finally, disinformation and misinformation likely increased distrust in traditional media (see table 4). The perception that the established media fabricated news to harm Bolsonaro’s credibility is a worrisome trend that did not cease after the campaign. This makes it harder for journalists to counter partisan information and government propaganda.

\section*{INSTITUTIONAL REACTIONS}

\subsection*{Government}

Brazilian authorities began mobilizing to address the challenges posed by disinformation as early as 2016. In 2017, Brazil’s Electoral Justice approved a resolution on election-related advertising that laid out specific rules for political advertising on the Internet and on social media.\textsuperscript{64} The resolution defined, for instance, that two types of advertisements on the Internet were permitted: the boosting of and sponsoring of links, such that a candidate or party’s content would become visible to a greater number of users. However, campaigns could only boost or sponsor links under two conditions: first, the content had to be identified as electoral content associated with a candidate or party’s content; second, the hiring of these types of amplifications online could only be done by a candidate or political party, or by their official representatives.\textsuperscript{65}

Before the elections, Brazil’s top electoral court

\section*{ITS Rio: Net Neutrality and Data Protection in the Fight Against Disinformation}

Ronaldo Lemos, Co-founder and Director, Institute for Technology & Society (ITS Rio)

\textbf{DISINFORMATION ONLINE IS A GLOBAL CONCERN AND one that stems from various factors. In Brazil, strengthening personal data protection is a way to prevent the misuse of personal data for political purposes, and to empower users to exercise more control in how their data is used for economic purposes. In Brazil, a General Data Protection Law was approved in August 2018. However, implementation of the law remains a challenge. As of March 2019, no final definition of the structure of Brazil’s Data Protection Authority existed. One concern is whether that authority will have enough independence from the government. Having an independent authority is an important element to establishing the compatibility of Brazilian law with the European General Data Protection Regulation.

Brazil took a long time to enact data protection legislation. As a result, enforcement of data protection in the country has been sporadic, and there is an overall absence of a data protection culture. As such, government databases have been made available voluntarily or leaked to private entities without deep scrutiny. Brazilians often find their personal data, including tax enrollment numbers, identity numbers, personal address, phone number and other sensitive information, freely available online in privately-owned but publicly accessible databases such as “Tudo Sobre Todos.” Naturally, this data ends up in the hands of political campaigns and disinformation actors, and at times is used by illicit actors for intimidation and coercion online. As of March 2019, Brazil’s data protection law comprised a loophole that enabled government bodies to freely transfer data to private entities, by means of a simple “partnership” (“convênio”) without further scrutiny or guidelines.

ITS Rio believes good data protection laws should help curb the abuse of personal data for the purpose of disinformation and other weaponized forms of communication in Brazil.
(TSE), in committing itself to standing strong against disinformation, created a group that gathered law enforcement and Internet specialists to discuss the issue. On August 22, then-TSE President Luiz Fux announced candidacies involved with “fake news” could be barred from running.66

During the campaign, however, the court failed to adopt strong measures against disinformation. The group met only six times, and not at all in the three months preceding the election. The new president of TSE, Rosa Weber, said she did not know what the former president had said about the issue and stated there was no “easy solution for the problem.”67

On the day of the first round of voting, fact-checkers criticized the TSE for failing to provide answers to their questions, which left rumors unanswered. Prior to the second round of voting, the TSE met with fact-checkers, and technology and social media companies, to discuss disinformation, resulting in the creation of a task force the weekend of the second round, during which time fact-checkers had contact with the legal and technology arms of the TSE.68

The court also launched a website to address rumors related to the electoral process.69 Notably, the TSE also responded to disinformation by ordering the removal of false accusations from the Internet, after being summoned by parties.70

At the state level, one of the electoral courts published one of the most effective debunking efforts of the election. An expert from the court analyzed a video depicting alleged fraud at a voting machine to prove it had been manipulated. The court was proactive in debunking the video, which had been shared by important politicians, including one of Bolsonaro’s sons.71

Finally, the Atlantic Council also observed that, due to alleged electoral law restrictions, state secretaries—the equivalent of state-level ministers—were not publishing information on their websites. Brazilian law prevents governments from publishing some information during the electoral period to prevent parties in power from using the government apparatus to benefit its candidates. There is, however, no consensus about what information can and cannot be published. In the case of Moa do Katende’s murder, the secretary of security of Bahia failing to publish any official information about the case online probably contributed to the spread of inaccurate information as this action prevented citizens who wanted to independently verify information from accessing statements from the official source.72

**Technology and Social Media Companies**

Ahead of the Brazilian elections, technology and social media companies took some action to address the challenges posed by disinformation. Facebook partnered with local fact-checking agencies, such as Aos Fatos and Lupa, to identify false information on the platform—the company worked to reduce the reach of posts classified as false by fact-checkers.73 Facebook also began labelling political advertisements and launched its archiving capability. Brazil became the second country after the United States where Facebook implemented these capabilities.74

Messaging platform WhatsApp, in June 2018, began labeling “forwarded” messages to clarify the original author of the message was not necessarily the person who shared it.75 WhatsApp also reduced the number of users with whom a person could share a message—from two hundred to twenty contacts (it would, following the election, further reduce that number from twenty to five). The messaging platform also partnered with fact-checking initiatives, including Comprova and ÉNóis. Along with these initiatives, WhatsApp internal investigations also resulted in the suspension of “hundreds of thousands” of accounts.76 It also reacted by implementing a campaign disseminated through traditional media and social media advising people about disinformation and advocating against the spread of disinformation and misinformation.
FGV DAPP: Brazil’s Election was a Turning Point for Social Media

By Marco Aurelio Ruediger, Director, Department of Public Policy Analysis, Fundação Getulio Vargas (FGV-DAPP)

Brazilians approached the 2018 electoral cycle sure of the impact of social media on politics, but still unsure about the level of effect it would have on shaping world views in both the short and long term. The key issue presented to those interested in deciphering the network society was whether almost real-time monitoring and more qualified analysis of social media would positively influence the political environment and favor a fairer (more informed and less polarized) election. This effort led to the creation of the Digital Democracy Room, #observa2018, by the Department of Public Policy Analysis at Fundação Getulio Vargas (FGV-DAPP), a pioneering initiative to monitor the public debate on the web and identify acts of disinformation, threats, and illegitimate interference in the political process.

Over the course of one hundred days, DAPP analyzed more than 130 million tweets and 163 million interactions on the Facebook pages of the thirteen presidential candidates and other key political actors, in addition to public data from Instagram and YouTube—the latter, a platform that proved to be increasingly important during the electoral race. The monitoring resulted in 123 analyses, with fourteen weekly reports, which contributed to discussions about the electoral process in both national and international press. The association of the macro themes monitored with the presidential candidates revealed that corruption was the most frequent subject discussed in debates about the election on Twitter. Following corruption, the network’s users were also concerned with public security and the economy.

In this vein, partnerships with organizations such as the Atlantic Council were essential to bring complementary methodological approaches to the forefront, and to address challenges along the way.

The presence of automated accounts was recurrent in this period—influencing up to 12.9 percent of the interactions on Twitter in the final week of the first round, according to FGV DAPP’s methodology. And these contributed to the spread of disinformation and misinformation both inside and outside of the country. Inflamed by the scenario of political polarization, disinformation was used as a campaign tool by all sides involved in the elections, reaching boundaries still unknown and, therefore, not fully understood. Such was the case of the WhatsApp platform, which was used as a vector for the spread of false information inside an almost untraceable environment—something that will certainly be a challenge in the coming years.

Monitoring done en masse during the electoral period indicates that social networks have become influencers of the political debate. Although this level of influence enables the amplification of arguments and actors, so effective action is necessary to ensure democratic institutions can continue to function properly and effectively.

DAPP points to the following as actions that can be taken to strengthen digital resilience and preserve democratic legitimacy:

- Social media platforms should accompany the observation of legal frameworks through electoral campaigns on the Internet and provide research centers with more access to data and efficient communication;
- The Electoral Court System should promote mandatory and continuous communication with social media platforms, empowering civil society organizations to monitor and analyze;
- The state and the civil society must obtain more knowledge, through the promotion of research, about the connection between public opinion and the social networks used during the 2018 Brazilian elections.

The 2018 Brazilian election was undoubtedly a major turning point for the impact of social media on political processes. Therefore, democratic societies must work to better understand the phenomenon, to avoid the corrosion of traditional institutions by disinformation and the misuse of technology.
Fact-checking Agencies and the Media

At times in partnership with technology and social media companies, fact-checking organizations and the media also mobilized to address disinformation and misinformation around the elections. A group of twenty-four media outlets came together to form the fact-checking initiative Comprova, spearheaded by the journalism non-profit First Draft, which functioned in a decentralized manner, with fact-checkers working from their newspaper’s offices. WhatsApp granted Comprova access to the messaging platform’s application programming interface (API), enabling the group to receive from the public questions about messages they suspected to be false on an intermediary website—with access to the API, the messages Comprova received went to a server, and not to a phone, facilitating the debunking process. Comprova published their verifications on their website and on social media, and replied to users who sent false messages to the fact-checking service with the verification of the message the user sent.

Globo, Brazil’s leading media group, also carried out a fact-checking effort, “Fato ou Fake” (Fact or Fake), that comprised all outlets belonging to the group. A joint effort, established during the weekend of the second round of voting, also brought together the country’s main fact-checking agencies: Aos Fatos, Lupa, Boatos.org, E-farsas, Comprova, and Fato ou Fake. Together, they debunked fifty rumors in forty-eight hours. In parallel, fact-checking agency Aos Fatos introduced “Fatima bot,” a Twitter bot, also available on Facebook Messenger, that replied to and alerted users when posts they shared online were inaccurate.

At least three initiatives in Brazil took fact-checking to WhatsApp: Aos Fatos, ChecaZap and O Poder de Eleger. The three organizations crowdsourced possibly false information from users, who submitted these by send them to the organization’s WhatsApp numbers. After fact-checking some, the organizations sent the results of the verification back to users via broadcast lists of up to 256 subscribers each on WhatsApp.

Despite their efforts, fact-checkers and the media encountered various challenges in their efforts to address disinformation. For one, these stakeholders were not always able to disseminate their verifications to the audience sharing false claims. The gap...
between audiences consuming disinformation and those sharing verified content can in part be attributed to Brazilians increasingly getting their political information from WhatsApp, rather than from independent news websites. Although various Brazilian fact-checking organizations asked users to send the organizations messages they had received on WhatsApp they suspected could be false, many of the organizations debunking disinformation did not publish their findings directly on WhatsApp, but rather on their websites or social media. This gap also existed on traditional social media platforms. Atlantic Council findings showed that when Bolsonaro was stabbed, for example, debunking efforts did not reach the same groups that shared inaccurate information about the incident on Facebook.

Another major challenge for these organizations was assuring they were not further amplifying disinformation, as they risked sending verified information to people who had not heard the rumor in the first place.

Civil-society Organizations and Academic Institutions

Civil society and academic institutions were pivotal in the fight against disinformation during the Brazilian elections. The Eleições Sem Fake project, for example, led by the Federal University of Minas Gerais (UFMG), was an initiative that created a way for media to have a glimpse into what was being shared within public groups on WhatsApp. Using automated scripts, the UFMG team identified and monitored 350 public groups on WhatsApp. Eleições Sem Fake gave data access to fact-checkers and the media, but did not publish personally identifiable information about group members. Nevertheless, WhatsApp expressed concern about researchers joining public groups without explicitly identifying themselves as researchers. Many think tanks and NGOs also analyzed Facebook, Twitter, and WhatsApp, while others tackled freedom of expression discussions or approached disinformation from the legal side. ITSRio was especially important in finding evidence of automation on WhatsApp groups.

LOOKING AHEAD: BRAZIL

Brazil's 2018 election cycle exposed the array of challenges disinformation and misinformation can pose for legitimate, fact-based political discourse, and the effects inauthentic online behavior can have in decreasing public trust in institutions. The election cycle also showed disinformation can have the power to set the agenda for political debates and news coverage. In 2020, Brazil will elect representatives in more than 5,000 municipalities—disinformation and misinformation are likely to emerge.

The next two years will lay the groundwork for stronger digital resilience in Brazil. In 2019, Brazil’s Supreme Court will rule on two cases that can set important precedents in the mobile-first country regarding encrypted messaging platforms. Some civil-society organizations hope the court’s decisions will support encryption and Brazilians’ rights to privacy.

Acknowledging the importance of encryption, nonetheless, does not preclude technology and social media companies from continuing to recognize and address the ways their platforms have been and could be used by illicit actors as vectors for the spread of disinformation. Technology and social media companies, as well as encrypted messaging platforms, must continue working with fact-checking organizations, the media, and electoral authorities to prevent the spread of disinformation in Brazil’s next election cycle.

Brazilians will also look to media to adapt based on lessons learned from 2018. Since the elections, independent news outlets have moved in a promising direction, not only by continuing to debunk false information but also by focusing on trying to explain disinformation. The Bolsonaro administration’s comments about the legitimacy and independence of media, however, may impact the level of trust Brazilians place on professional news organizations, and could affect how verifications of disinformation and misinformation are perceived by the population in the next election cycle.

Finally, the emergence of hyperpartisan media—with fringe outlets acting to spread hyperpartisan, opinion-based viewpoints, rather than taking on the role of independent watchdogs—has the potential to negatively shape the way citizens engage with politics.

With Brazilians more aware of the existence of disinformation and misinformation, stakeholders from electoral bodies to technology and social media companies should continue working to address these challenges. On an individual level, voters can continue to question and verify narratives and to strengthen their digital resilience from the moment they get online.
On July 1, 2018, Andrés Manuel López Obrador (AMLO) was elected president of Mexico after forging the “Together We Will Make History” coalition, composed of the new National Regeneration Movement (MORENA) party, the Labor Party (PT), and the Social Encounter Party (PES). AMLO’s 2018 victory was both historic and record-breaking—historic for its defeat of the traditional political parties, and record-breaking because it was the first time a president received almost 54 percent of votes, attributed to record-high levels of turnout. More than 59 percent of Mexico’s eligible electorate came out to vote. AMLO, who served as mayor of Mexico City from 2000 to 2005, had run for president in 2006 and again in 2012. With an unprecedented lead over the runner-up candidate Ricardo Anaya from the National Action Party (PAN), López Obrador’s resounding victory shook the political establishment. As of February 1, 2019, he had an approval rating of 86 percent.

The 2018 elections were also the biggest in Mexico’s history. Over 18,000 seats—629 at the federal level and more than 17,500 at subnational levels, including nine governorships—were up for grabs. The elections were also the most violent: electoral authorities in Mexico registered a total of 774 aggressions against politicians. One hundred and fifty-two politicians were murdered, 48 of which were pre-candidates and candidates running for office. According to the Specialized Attorney for the Attention of Electoral Crimes (FEPADE), between January and September 2018, law enforcement initiated over 1,062 investigations of election-related crimes. Guaranteeing the safety and security of candidates ahead of future elections will be key to assuring the integrity and legitimacy of future votes.

**KEY FINDINGS**

- Disinformation in Mexico’s elections comprised primarily automation and artificial amplification, rather than organic disinformation.
- The hiring of commercial bots for financial gain, the use of political bots for the spread of specific electoral messages, and disinformation about the electoral process at the state level stood out as the three most worrisome trends of disinformation around Mexico’s elections.
- Verificado 2018, in uniting a network of journalists, civil society, and other organizations under a central hub and one single brand, generated significant impact in promoting transparency and accountability. The model should be replicated ahead of other elections.
Modest Growth Rates, Deterioration of the Rule of Law, and Changing Trade Environment

Years of modest economic, a deterioration in the rule of law and individual security, and uncertainty around the fate of the North American Free Trade Agreement (NAFTA) renegotiations during the campaign cycle created new openings for an outsider to enter the political fray. In the span of two years, from 2015 to 2017, Mexico dropped forty places in Transparency International’s Corruption Perception Index. In Latin America, the same index ranked Mexico higher than only Guatemala, Nicaragua, Venezuela, and Haiti. Regarding violence, the 2018 murder rate of more than thirty-three thousand homicides was a 15-percent increase from 2017, and constituted the highest homicide rate in modern Mexican history. Mexico is also the second-most dangerous country for journalists, second only to Syria in 2017. In 2017, Article 19 registered 507 aggressions against media and journalists, and twelve deaths directly related to journalistic activities. The job of the media remains dangerous in Mexico—as of February 22, 2019, a total of fourteen activists had been killed from the time AMLO took office.

AMLO’s victory can be attributed to a successful campaign aimed at resolving these systemic problems plaguing the country. His focus on Mexico’s rampant corruption and rising crime rates resounded with millions of disenchanted voters. But AMLO can also attribute his win to his campaign’s adept use of social media. Presidential candidates allocated approximately 25 percent of their budgets to online outreach, up from only 5 percent six years before. AMLO spent less money when compared with his adversaries, spending 85 million pesos, compared to Ricardo Anaya’s 338 million and Jose Antonio Meade’s 302 million. Even with the disparity in money spent, AMLO dominated the conversation on social media platforms like Twitter, where 40 percent of all Tweets about the election mentioned him, while his rivals were under the 20-percent mark.
INFORMATION AND ELECTION ECOSYSTEMS

Whereas in Brazil disinformation was mostly organic in nature, in Mexico automation and artificial amplification of messages permeated information channels during the 2018 elections. To understand why this was the case, it is important to acknowledge how Mexicans consume information, as well as how the country’s electoral system functions.

Mexico’s Information Ecosystem

In a 2018 Reuters Institute survey, 90 percent of respondents chose “online” as their go-to source for news. The same report finds that 62 percent of respondents consume news through television, and 71 percent via social media, although trust in social media is low, at only 40 percent. In Mexico, there are over 80 million active Facebook users, and Facebook is the top social media platform used for news consumption (61 percent of respondents say they use Facebook).

As in past elections, social media played an important role in pre-electoral conversations and was therefore a natural target of digital manipulation. Unlike other Latin and South American countries, Mexico has one of the highest Twitter penetration rates in the world, which in 2018 stood at around 49 percent. The Reuters Digital News Report found that 23 percent of the Mexican population relied on Twitter as a source for news.

As such, the Atlantic Council found that online actors invested in creating and leasing botnets to amplify political messages.

Mexico’s Election Ecosystem

Voting in Mexico is mandatory. Anyone over the age of 18, with the exception of felons, can vote in Mexican elections. Every six years, Mexicans vote for president and elect the 128 senators and 500 members in the Chamber of Deputies. Midterms for the Chamber of Deputies take place every three years. Constituents vote directly for their candidate, and the candidate with the highest number of votes wins. Mexico’s nine predominant political parties are primarily financed through public funding, following a specific allotment procedure. To some extent, this funding structure helps create a level playing field; in addition, private funding may not exceed public funds. Effective coordination between national and local electoral authorities in Mexico is no easy task. Since 2014, the Instituto Nacional Electoral (INE) has been responsible for organizing elections by harmonizing standards and processes for local and federal votes, guaranteeing the electoral rights of citizens, and counting votes at the national level. The Federal Electoral Tribunal (TEPJF), created in 1990, is the highest authority on electoral matters. These are considered the “cornerstones of the Mexican electoral ecosystem,” involved in all aspects of elections.
The Atlantic Council’s #ElectionWatch Latin America effort in Mexico was conducted in partnership with media outlet Animal Político and fact-checking coalition Verificado 2018. A coalition of over eighty international, national, and local media organizations, civil-society organizations, research groups, and private companies, Verificado 2018 was born after the September 2017 earthquake in Mexico. It was inspired by Verificado19S, the collaborative initiative that came together within a context of disinformation around the earthquake to fill information gaps left by the government, to counter false information, and to connect citizens who needed help with those who were able to provide it. Verificado 2018 was created to address false information around Mexico’s election—the project was active throughout the electoral cycle and became a national entity that had to be responded to as it uncovered cases of disinformation and automation.

In Mexico, while the spread of disinformation by several actors—constituents, specialized media firms, presidential and local candidates, and others—certainly exploited existing political rifts and insecurities to amplify distorted narratives, disinformation around the election was marked most prominently by automation. Disinformation comprised manufactured, artificial dissemination that included both coordinated and automated amplification of narratives online. Particularly, automation comprised the use of bots and bot networks to artificially spread messages.

**Artificial Amplification of Content for Commercial Gain**

In Mexico, the Atlantic Council uncovered cases of a “diseconomy” of buying and selling social media engagements—likes, shares, and comments—for commercial gain. Researchers uncovered the use of the global market for false amplification to promote political or partisan content. On Twitter, this took the form of automated bots on Facebook, it consisted of commercial groups that coordinated large-scale responses to posts in return for payment.

The most egregious case concerned a Mexican entrepreneur, Carlos Merlo of Victory Lab, who claimed to control a network of millions of fake accounts on Twitter and Facebook. He claimed he used these networks to serve politicians and businesses for substantial sums (up to the hundreds of thousands of dollars). The Atlantic Council investigated his claims and demonstrated that Victory Lab was boosted by apparently commercial bots—bots whose activity can be rented out to anyone willing to pay for likes or reposts—from East Asia on Twitter, while its Facebook posts were liked by hundreds of accounts from South Asia and Brazil.

Partisan political messages during the election in Mexico showed a similar pattern of amplification. This does not definitively tie them to Victory Lab, but the mass liking of Mexican political posts by Indian and Brazilian accounts indicates false amplification purchased online. On Twitter, the Atlantic Council also observed amplification of political posts in Mexico by commercial bots that appeared to come from Russian-speaking accounts. The amplification was on a small scale, in the low hundreds of interventions. The accounts posting these retweets shared content in a wide range of languages and themes, indicating that they were most likely commercial bots for hire. Despite the Russian origin, there was no evidence to suggest that these were linked to a Kremlin influence operation, despite concerns and public statements from national security officials in the United States. Atlantic Council research found that interventions were connected to commercial accounts, and on too small a scale to suggest a state-backed campaign. This is more likely to have been a case of an individual buying amplification online.

**Bots Amplifying Political Content**

The Atlantic Council also uncovered examples of bots amplifying narratives to impact election results. Some political parties utilized political bots—bots created to amplify one political message or stance.

One such case showed the use of political bots in the state of Puebla, where a small yet hyperactive network of bots was amplifying content from two PRI party candidates running to represent the state of Puebla—PRI senator candidate Juan Carlos Lastiri Quiros and PRI gubernatorial candidate Enrique Doger. Unlike commercial bots, which promote a variety of brands and services in addition to politicians, the Puebla bots promoted the two candidates and the PRI party’s campaign materials exclusively.

The bot accounts were created between May 8 and May 16, 2018, and had their location set to the state of Puebla. This was the first indicator the accounts were political, not commercial (a commercial bot can be used for political purposes, but a political bot is created for the sole amplification of political messages), as political bot herders tend to assign the bots locations where the candidate, or the party they are promoting is running to guarantee the content promoted by the bot accounts trends within that constituency. The bots used by the PRI party in Puebla were...
Disinformation in Democracies

...relatively sophisticated. They operated in small numbers and refrained from posting repetitive posts to avoid Twitter’s spam detection. While the bot activity created a false sense of engagement, it failed to influence the election outcome, as neither of the two candidates won their respective seats.

The bot activity continued until election day. The Atlantic Council discovered that three days before the election, pro- and anti-AMLO bots were arguing on Twitter under a pro-AMLO hashtag #AMLOFest. The anti-AMLO bots amplified a video called “AMLO’s Dark Secret,” which falsely accused the candidate of murdering his own brother and best friend. The bots on both sides were highly active, with as little as ten bots posting more than one thousand tweets in a matter of hours.

The bots managed to stifle the organic conversations under the same hashtag, illustrating their broader capacity to stifle free speech, not by suppressing it, but rather by drowning it out with automated messages and activity.

Disinformation Regarding the Electoral Process and Claims of Electoral Fraud

Local elections in Mexico registered high levels of violence and various electoral irregularities—in some cases, electoral authorities nullified elections or called for vote recounts as a result.

The gubernatorial election in the state of Puebla was the most salient case. On election day, Puebla registered high levels of violence, with reports of people murdered and ballots stolen or set on fire. Following a close race between the two leading candidates for governor, electoral authorities announced official election results would be delayed by several days.

On that occasion, the Atlantic Council reported that bot-like users tried to influence and promote misleading information about the electoral process on Twitter. These bot-like accounts promoted a series of hashtags to encourage the victory of one candidate despite official results not having yet been made public. The hashtags promoted included #PueblaEligióPAN and #YoVotéXMarthaErika in favor of Martha Erika Alonso as the elected governor of Puebla. In response to the latter hashtag, the bot-like accounts also promoted #YoNoVotéXMarthaErika in support of Miguel Barbosa, the other contender.

Two and a half months after the elections in Puebla, and with more than 500 complaints of electoral irregularities, Mexico’s highest electoral court demanded a recount of the votes. While the vote recount was under way in Mexico City, the Atlantic Council again observed bot-like accounts promoting the victory of one of the leading contenders over the other during the vote recount, before electoral authorities released official results.

The Puebla battle on social did not stop once electoral authorities released the final results. It was further exacerbated following the death of Martha Erika Alonso and former governor Rafael Moreno Valle in a helicopter crash, when hashtags emerged on social media claiming the crash had not been accidental.
Verificado 2018: A Model in the Fight Against Disinformation

By Tania Montalvo, Executive Editor, Animal Politico and Coordinator, Verificado 2018

MEXICO'S 2018 ELECTIONS WERE THE largest in Mexico's history. With 3,400 political posts up for grabs, the digital world became a key battleground in the fight for votes, and disinformation became a popular tool to engage the over sixty million Internet users and thirty-five million WhatsApp users who rely on digital platforms to receive and exchange information.

In response to this reality, a group of journalists developed Verificado 2018, a collaborative effort that put citizens at the core of electoral and digital debates. Verificado 2018 took inspiration from ElectionLand in the United States and CrossCheck in France, both of which brought media together to fight disinformation.

Verificado 2018 embodied a new model of collaboration. Comprised of a central working group that later became a news agency for more than eighty allies, Verificado 2018 enabled all members to work under one brand that conveyed a message of unity in the fight against disinformation: a group of allies working to promote informed voting.

Thanks to the large network and common brand Verificado 2018 created, Mexican national and local television stations, broadcasters, and print media, as well as digital media, picked up and broadcast the group's content nation-wide.

What did Verificado 2018 achieve? Verificado.mx registered 5.4 million visits to its four hundred published entries. This number does not take into account information published by Verificado members, meaning the impact was likely much greater. On AnimalPolitico.com, for example, Verificado 2018 posts garnered almost ten million visits. Verificado 2018 was also able to engage voters through different channels. For two months, the group's WhatsApp number brought in a total of 9,600 subscriptions and 60,700 interactions.

Verificado 2018 saw disinformation change throughout the electoral process as the public debate shifted. At the start of the campaign, for example, disinformation was directed at Andrés Manuel López Obrador (the Movimiento Regeneración Nacional (MORENA) candidate and leading contender) and José Antonio Meade (the incumbent government's candidate). After the first presidential debate, when polls and opinion leaders indicated Ricardo Anaya (the Partido Acción Nacional and Partido de la Revolución Democrática (PAN-PRD) Coalition candidate) could win the race, disinformation about him began to surface while disinformation about Meade decreased. López Obrador, who led in the polls throughout the campaign cycle, remained the primary subject of false news, from both opposition groups and supporters, who created and disseminated false information in his defense. As election day approached and López Obrador continued to lead, disinformation shifted to the voting process and Mexicans' right to vote: how to vote, where to vote, what constituted an electoral crime, and alleged prohibitions at voting booths.

We cannot know for sure how disinformation affected the candidates, but we know Verificado 2018 affected how disinformation went viral and the way in which readers interacted with it: at the beginning of the project, each piece of disinformation would garner around 150,000 shares while at the end, days before the election, it was hard to spot pieces of disinformation that had been shared that many times.

Verificado 2018 showed that collaboration must underpin the fight against disinformation. The initiative highlighted the importance of carrying out the fight against disinformation on multiple fronts, and of employing different formats and communication channels.

Disinformation in Mexico continues. Today, it is not only focused on politics but also on social issues, and it constitutes a discourse of hate. The next step will be to reinforce the effort initiated by Verificado 2018, to prevent disinformation surrounding materials that explain disinformation's consequences and involve citizens. It is not enough to say that a piece of information is false—we must show the effects of disinformation and share with citizens the responsibility of creating and consuming quality content.
Foreign State-Funded Media Outlets

A head of Mexico’s presidential elections, then US National Security Adviser H.R. McMaster warned that the Russian government had launched a campaign to influence the country’s elections. As part of the Atlantic Council’s #ElectionWatch research into potential Russian influence in the Mexican elections, the team looked at Russian-funded media outlets publishing in Spanish to determine if any were trying to influence the vote. The Atlantic Council analyzed the coverage of the elections in Latin America across Kremlin-funded media outlets such as RT, Sputnik, and News Front, as well as the pro-Kremlin website globalresearch.ca. Although these outlets covered the Mexican elections and had a strong anti-US bias, none demonstrated explicit bias toward particular parties or candidates in Mexico.

Encrypted Messaging Platforms

Although in Mexico Atlantic Council research focused primarily on Twitter, a platform with which Mexicans consume information at high rates, messaging platforms such as WhatsApp remain an important source of information; according to a 2019 survey, approximately 17 percent of Mexicans spend at least six hours per day on the application. The true scale of disinformation campaigns on encrypted messaging platforms cannot be fully measured, but Atlantic Council research shows that content shared on WhatsApp is often reflective of content shared on open social networks such as Facebook and Twitter. In Mexico’s case, more research is needed ahead of the country’s next elections to determine how narratives form and are spread on WhatsApp.
IMPACT ON THE ELECTIONS

Although the influence of disinformation and automation on voter decisions is difficult to measure, the following analyses based on Atlantic Council case studies published over the course of 2018 paint a picture of the impact of disinformation and automation on Mexico’s elections.

National Level: Little Discernible Impact

Most artificial amplification observed during the campaign period comprised attacks on AMLO, the winner of Mexico’s presidential election. AMLO’s significant victory across gender, age, and education levels—especially among highly educated (university level or up) men aged 26-35—showed it is unlikely online disinformation and automation attacking him significantly impacted the results of the election at the national level. The most likely impact of disinformation and artificial amplification online was of a financial nature and affected individual politicians—Mexican media reported that entrepreneurs like Carlos Merlo and others potentially charged politicians hundreds of thousands of dollars for covert social media campaigns.

State Level: Local Unrest

At the local level, particularly in the states in which election results were contested or had a higher number of irregularities, disinformation and inauthentic engagement efforts focused on undermining the legitimacy of the electoral process and the credibility of electoral bodies. In the case of Puebla, amid a vote recount, disinformation and artificial engagement on social media reflected polarization and exacerbated existing tensions between opposing political groups. This became more evident following the death of Martha Erika Alonso, when new conspiracies about the nature of the helicopter accident emerged online.

Party Level: Political Parties and Governments

Atlantic Council research indicated political parties in Mexico at times turn to artificial amplification to bolster support for their political campaigns and candidates. According to local journalists with whom the Atlantic Council spoke, some political marketing companies also include these types of services in their proposals to political parties and government.

As was seen with the government of the state of Oaxaca in southern Mexico, governments at times resort to bot-like and artificial support to promote their image. The Atlantic Council identified farm-like accounts promoting social media pages from the Oaxaca state government—an Atlantic Council analysis of online patterns of engagement in Mexico uncovered an unusual number of South Asian accounts reacting to posts on the official Facebook page of Alejandro Murat Hinojosa, the governor of the state of Oaxaca, in southern Mexico. Similar
reactions can be seen on his official state government’s page and Guelaguetza page—an account intended to promote the Guelaguetza festival, an annual traditional indigenous festival celebrated in the city of Oaxaca every July.

The very high proportion of South Asian reactions is unusual for Spanish-language political content in Mexico. The proportion and number of likes—in comparison to Facebook’s other options of loves, laughs, and angry reactions—also appeared distorted. Both features suggest that the “like” reactions were obtained from South Asia as part of a transaction, most probably in return for payment. Nonetheless, it is important to state that this does not suggest the South Asian likes were paid for with taxpayers’ money nor that government authorities were responsible for this.

Additional research is needed to determine whether political parties and government actors are actively engaging in artificial promotion of their platforms and activities on social media. Nonetheless, open-source research suggests political parties and governments are making some use of these strategies.

INSTITUTIONAL REACTIONS

Government and Technology and Social Media Companies

As Mexico’s electoral authorities sought to address the challenges of disinflation in the elections, debates emerged about the balance between regulation and freedom of speech. When Mexico’s Tribunal Electoral del Poder Judicial de la Federación (TEPJF) was established, disinflation online did not exist to the same extent it does today. Reactions and rulings from the TEPJF thus need to thread a fine line to remain in the parameters of its constitutional mandate, and to assure actions to stop illicit activity online do not also open doors for infringement on freedoms of expression.128

Furthermore, there is still a lack of clarity on how technology and social media platforms can be used during the different phases of the electoral process, whether it be throughout the campaign process, the day of the election, or in the post-electoral phase.

Fact-checking Agencies and the Media

The fact-checking initiative Verificado 2018 in Mexico was perhaps the most successful in countering disinformation and misinformation, and shedding light on automation, around elections in Latin America. Over eighty media outlets—spanning international, national, and local media—joined the effort to raise awareness of and fact-check false information, the biggest collaborative effort of its kind. Civil-society organizations and academic institutions also took part. The initiative, inspired by a crowdsourced effort to map available resources in Mexico City following a massive earthquake in September 2017, drew also upon crowdsourcing and volunteers to help verify information and debunk hoaxes in real time. The project received funding from Open Society Foundations, Oxfam, Facebook, Twitter, Google News Lab, and Mexicans Against Corruption and Impunity, among others, and oversaw the Mexican information environment over the course of four months.129

Verificado 2018 systematically documented and exposed false content, something that had never happened at scale in Mexico’s history. The group’s unique model, which comprised a central hub and enabled members to work collaboratively under one brand to debunk false news and guarantee informed voting, helped to promote confidence among voters about the veracity of candidate statements throughout political campaigns, as well as the legitimacy of election results. The group also published educational and informational material to help constituents understand phases of the electoral process.130

Whereas in other countries fact-checking organizations and media worked from their own newsrooms and with no central command structure, Verificado 2018 became in Mexico an active body that elicited responses from candidates and other political stakeholders. The group was also a central part of the election conversation.
Civil-society Organizations and Academic Institutions

Civil society and academic institutions in Mexico, including Mexico Como Vamos, Think Tank New Media, Article 19 and others also participated in the Verificado 2018 effort. In addition, Mexico’s civil society and academia sought to discuss and address issues of disinformation through conferences and studies leading up to election day. Academics from Universidad Iberoamericana (Iberoamerican University), the Instituto Tecnológico y de Estudios Superiores de Monterrey (Monterrey Institute of Technology and Higher Education), the Centro de Investigación y Docencia en Económicas (Center for Research and Teaching in Economics) as well as international experts from the National Democratic Institute, the Institute for the Future, and the Center for Research, Transparency and Accountability took part in various conferences, alongside INE and the media, leading up to the elections.

LOOKING AHEAD: MEXICO

It is unlikely the pace of automation in Mexico will slow before the country’s 2024 presidential election cycle. In fact, disinformation and automation will likely remain vehicles for digital exploitation over the coming months and years, not only in elections, but around social issues.

The 2018 election cycle in Mexico demonstrated how bots can take control of a conversation at high rates and on a broad scale. The fight against disinformation and automation is an up-hill battle—as one instance of automation is uncovered and addressed, others emerge. Global technological developments in Artificial Intelligence will increasingly make identifying robotic activity at scale and distinguishing citizens from bot accounts more difficult, with enormous implications.

Verificado 2018 played an important and unique role in Mexico’s fight against disinformation and misinformation before and during the elections. In collaboration and under the umbrella of one brand with a central hub, the group brought disinformation and misinformation, and the challenges associated with these illicit activities, to the forefront of public debates.

The efforts Verificado 2018 spearheaded around the last elections will become increasingly necessary. Given the complexity of disinformation, more civil society organizations, academic institutions, and government agencies are likely to join the ranks of a Verificado-like project around 2024.

A multi-stakeholder approach to strengthening digital media literacy for public officials as well as for voters, in a country where online news as the go-to source is rapidly gaining market share, will be key in protecting the integrity of the digital information environment ahead of future elections in Mexico. Digital media literacy and the ability to adequately respond to disinformation will be key in combatting efforts that aim to undermine the credibility of electoral bodies and the legitimacy of the electoral process.

In Mexico, disinformation and automation will likely remain vehicles for digital exploitation over the coming months and years, not only in elections, but around social issues.
COLOMBIA

By Jose Luis Peñarredonda and Roberta Braga

KEY FINDINGS

Disinformation in Colombia’s elections largely comprised organic disinformation at times amplified by media outlets and political leaders.

In a polarized electoral environment, fact-checking organizations and the media must work to assure verifications reach the same audiences exposed to and affected by disinformation.

As in the case of Brazil, countering disinformation narratives, rather than instances of disinformation, may be more effective in assuring that disinformation does not set the agenda for electoral debates and media coverage.

CONTEXT

On June 17, 2018, Colombians elected Iván Duque Márquez as their next president with 54 percent of the vote after two highly contested rounds of voting. Four months earlier, the country had elected the one hundred and eight senators and one hundred and seventy-one representatives who would serve in Congress for the next four years. In both contests, three concerns that transcended borders permeated the electoral process: the effects of disinformation and misinformation on election results; the impact of high degrees of polarization in political discourse, and the consequences of citizens’ lack of knowledge or lack of trust in the electoral process.
Evidence of disinformation campaigns previously emerged around the 2016 plebiscite on Colombia’s peace agreement with the Revolutionary Armed Forces of Colombia (FARC). A worrying precedent was set at that time about the potential effects of disinformation on political discourse. The victory of the “No” camp, a vote against the peace agreement, by little more than 50,000 ballots (0.2 percent of the total) was partly attributed by academics, the media, and non-governmental organizations to a seemingly organized disinformation operation conducted through WhatsApp and other social media platforms by some sections of the opposing right-wing campaign.\textsuperscript{131,132,133} In an interview days after the vote, its manager, Juan Carlos Velez Uribe, acknowledged a strategy of distortion of the facts.\textsuperscript{134}

During that referendum, the flow of organic disinformation through family and friend groups on WhatsApp, many of them false or out of context per a study conducted by a researcher at the University of Santiago de Compostela in Spain, was considered to be a contributing factor to a surprising outcome, since most polls forecasted a wide margin of victory for the “Yes” vote.\textsuperscript{135} This generated increased awareness about the risks misinformation and disinformation represented for the integrity of the 2018 presidential elections, and government, media, civil society and technology companies ramped up their efforts to create awareness of disinformation and misinformation among the public and to better understand their effects.

The outcome of the plebiscite became one of the most significant topics of political debate following the peace deal referendum in August, and fueled polarization in the country. In spite of having said that “Colombian people [...] will have the last word,”\textsuperscript{136} then-President Juan Manuel Santos made some changes to the peace deal after a brief consultation with opposition parties, and Congress approved it. The Centro Democrático party, as well as some sectors of the Conservative Party of Colombia, continued to aggressively oppose the deal once implementation fell to Congress, while the political center and those on the left were largely satisfied with it moving forward. This situation gave way to hyper-polarization during the presidential campaign.

The two top candidates in the presidential election belonged to opposing sides of the political spectrum and represented the two sides of the 2016 plebiscite.
discussion. Iván Duque identified with the conservative policies aligned with former president Álvaro Uribe, while Gustavo Petro, former mayor of Bogotá, championed a more left-leaning agenda. The third runner-up, Sergio Fajardo, led a center coalition that agreed with the peace agreement but promoted more pro-open-market policies than did Petro.

Leading candidates Duque and Petro represented two starkly different visions for the country. While Duque ran on a platform underpinned by opposition to the peace agreement for its alleged leniency with the FARC’s top ranks, Petro was a keen defender of the peace deal, and advanced a “progressive” agenda. These different approaches to the way forward for peace and the country’s future created an environment that enabled the spread of disinformation around the elections.

Lack of Institutional Trust

The 2018 election took place within a climate of widespread public distrust in the country’s institutions, particularly in the organizations responsible for monitoring elections. According to a 2017 study conducted by the Institute for Democracy at the Universidad de los Andes, 31 percent of Colombians are satisfied with the way democracy works in the country, around 24 percent trust elections in the country, and 10 percent trust political parties, “a trend that coincides with the increasing disapproval toward the operation of Colombian democracy and its most representative institutions.” Absenteeism remains widespread. In the runoff for the 2014 presidential election, only about 48 percent of qualified voters cast a ballot, and congressional and regional elections saw even worse turnout.

This lack of trust exacerbated disinformation and misinformation narratives during the presidential elections. Electoral institutions and media often found themselves caught in the middle of the crossfire of a belligerent political debate, and—despite their efforts—were limited in their ability to effectively counter false narratives and disinformation about the neutrality and reliability of their own work.

INFORMATION AND ELECTION ECOSYSTEMS

To understand how disinformation and misinformation spread during the 2018 elections in Colombia, it is important to understand not only Colombia’s information environment, but also the institutions responsible for managing elections.

Colombia’s Information Ecosystem

According to official government statistics, around 75 percent of Colombians used the Internet at least once in 2017. Of those who use the Internet, around 87.5 percent use Facebook, and 87.3 percent use WhatsApp. Of those
on WhatsApp, nearly 93 percent open the app daily. As a result, politicians increasingly use digital media and communications for campaign purposes; and some have been responsible for spreading disinformation. In 2018, all presidential candidates had an active and official presence on Facebook, Twitter, and YouTube. In addition, a number of social media groups, pages, or accounts supporting individual candidates—sometimes grassroots, and sometimes run by political parties and organizations—sprouted during the electoral campaign.

Polls conducted by advertising agencies since 2017 show that social networking services like Facebook or Twitter are the most frequently used platforms for the consumption of news after television, with nearly half of Colombians saying they use the platforms to do so. Surveys also place the popularity of social media above online news media, radio, and print media.

While Colombian audiences increasingly rely on social media over traditional media for information, electoral authorities and legislations have not yet caught up to address the changing media environment. Media regulation around elections were instituted in a pre-social media era, making it particularly difficult for the appropriate authorities to tackle information distortions online.

**Colombia’s Election Ecosystem**

Three elections took place in Colombia in 2018. Congressional elections occurred in March, as did primaries for the Centro Democrático Party and Petro’s Progresistas movement, which Duque and Petro won respectively. The first round of presidential elections took place on May 27, and the second on June 17. None of the three elections, nor the August 26 referendum on anti-corruption measures, generated a turnout higher than 53.7 percent.

Voting is not mandatory in Colombia but is incentivized by benefits that include discounts on requests for expedition of passports and public university tuition.

The main institutions in charge of organizing and guaranteeing the integrity of elections in Colombia are the National Registry of Civil Status (RNEC, Spanish acronym) and the National Electoral Council (CNE, Spanish acronym).

The RNEC issues national identification cards to all Colombian citizens and maintains the “electoral census,” a list of all citizens able to vote: everyone over 18, except for convicted felons, enlisted members of the military, and the police. The RNEC is also responsible for setting up polling stations throughout the country and in Colombian consulates worldwide, recruiting electoral jurors for polling places, and conducting a first count of the results after the election. The CNE is the highest electoral tribunal in Colombia. It has the last word on election results and oversees investigating and sanctioning infractions to electoral jurisdiction.

---

**Linterna Verde: WhatsApp Was Not the Beginning, Nor the End of Misinformation in Colombia**

Carlos Cortés, Co-Founder, Linterna Verde

**WHEN IT CAME TO DISINFORMATION AROUND Colombia’s 2018 presidential election, Linterna Verde found that encrypted messaging platforms like WhatsApp did not have an independent or isolated impact on elections. In Colombia’s information space, the encrypted messaging platform was complementary and parallel to open social networks such as Facebook and Twitter. In that sense, disinformation was not exclusive to WhatsApp, and it did not mark the beginning nor the end of attempts to manipulate election conversations.**

Our research did find that presidential campaigns have the capacity to undertake disinformation operations. Although we cannot say that campaigns took steps to insert content onto WhatsApp, the campaigns’ infrastructure and operations offer powerful incentives for them to be a source of, or point for, reinforcing false or manipulated narratives. Campaigns have databases, community managers, designers and—of course—computers, all working to implement communication strategies. In that regard, and as a couple of sources told Linterna Verde, although those assets are used for legitimate actions, they can, at times, also be used to advance disinformation on social media.

WhatsApp’s usage in Colombia has evolved with social practices. Linterna Verde’s research found that voters increasingly tend to reject unsolicited political campaigning and activism on WhatsApp. In that sense, successful attempts to manipulate and disinform require articulated operations on the ground. With such influence, WhatsApp can indeed reinforce environments for manipulation and radicalization.
There are eleven “electoral offenses” in the Colombian criminal jurisdiction, including fraud, voter impersonation, and disturbance of the elections. “Electoral coercion,” or making someone vote in a given way by means of “a deceitful maneuver” is punishable by at least four years in prison. They are prosecuted by the Office of the Attorney General and ruled on by criminal judges.

Several laws regulate media and political communication during elections. Candidates must declare all media and advertising expenditures, as these are considered campaign expenses and therefore count against spending limits. Political advertising in media and on the streets, polling, and public meetings are banned for two days before the election.

Colombia’s regulatory framework around elections, while robust, remains insufficient for addressing the challenges a changing digital communication environment can pose to the integrity of an election process. Laws currently in place do not prevent unofficial political campaigning that happens on social media, nor polling conducted by social media users. Since the framework requires that only campaigns declare expenses; individual users have no barriers or limits to unofficially paying for and disseminating advertising messages in support of a candidate online.

The regulation criminalizing coercion also seems insufficient for prosecuting online disinformation and misinformation, as it requires that the prosecutor prove a person voted as they did because of false information produced by the defendant. In this sense, the difficulty in demonstrating that someone would have voted differently if they had not been in contact with disinformation or misinformation online is a significant obstacle in prosecuting such crimes.\(^{143}\)

However, any strengthening of this regulation would have to be carefully measured against its potential consequences for democratic liberties such as freedom of speech or privacy. Balancing between these two imperatives is perhaps the biggest challenge for legislators and media, and for regulators in Colombia and elsewhere.

**DISINFORMATION AND MISINFORMATION IN THE 2018 ELECTIONS**

To explore how disinformation played into public discourse and impacted electoral outcomes in Colombia, the Atlantic Council’s Digital Forensic Research Lab and Adrienne Arsht Latin America Center conducted open-source investigations and published articles explaining cases of disinformation and misinformation in real time.

Disinformation and misinformation on social media were common throughout the 2018 election. During the presidential campaign period (March 12 to June 16), Colombian fact-checking organizations received daily requests to verify allegedly false claims.\(^{144}\)

In Colombia’s case, polarization seemed like the biggest driver of disinformation and misinformation during the presidential campaign. #ElectionWatch research in Colombia—done in partnership with La Silla Vacía, Lintern Verde, and Centro Gabo—showed the prominence of organic disinformation and misinformation in Colombia, fueled by polarization and often amplified by high-level political representatives,
and at times news outlets. At the same time, a handful of new, highly partisan media outlets, Facebook groups and pages, and Twitter profiles, drove significant engagement and traffic by catering to audiences engaged on both ends of the political spectrum, often by offering partial or blatantly false accounts of the news. Atlantic Council #ElectionWatch Latin America findings, as well as other researchers’ results, also indicated disinformation circulated prominently on the messaging app WhatsApp, one of the primary tools for communication in the region.

### Polarization and Amplification of Disinformation by Elected Officials

Through open-source investigations conducted before, during, and immediately following the two rounds of elections between May and August 2018, the Atlantic Council found that verified and non-verified social media accounts of political leaders, candidates and political parties of all political leanings were among the main amplifiers for the spread of false or misleading content online.

#ElectionWatch case studies published during the election cycle consistently showed political leaders and their online accounts as major sources and amplifiers of disinformation. They directly started or helped distribute false or misleading claims that advanced or solidified their positions. In one instance, Petro’s social media accounts amplified an accusation of electoral fraud against him during the first round, when some voters claimed amendments and corrections had been made to E-14 forms, the documents on which polling officials write how many votes each candidate had at each polling station. This piece of disinformation was amplified after the candidate retweeted the claim to his followers. The claims were not of a scale large enough to be substantial and were based on a misunderstanding about the electoral process. Still, they spread very quickly on social media, in part because they played along a narrative of mistrust of authorities that suited Petro’s anti-establishment rhetoric. He used the episode to push his campaign: he briefly called for a protest “if there was evidence of a fraud.”

E-14 forms are filled out manually and are the first step in a complicated vote count that lasts several days before results are made official by the National Electoral Council, Colombia’s supreme electoral authority. The forms are scanned and published online and are freely accessible for the public to scrutinize. In this case, the National Registry explained that the main issue stemmed from the existence of three different E-14 forms: one used to transmit preliminary results on election day, another scanned and published on the National Registry website, and another used for the official vote count. The process provides for handwriting mistakes in the E-14 forms, and inconsistencies are corrected at a later stage. Hence, the fraud claim was based on a minority of transcripts that were going to be corrected. Colombian NGO Electoral Observation Mission (MOE being the acronym in Spanish) verified this through an independent study, which showed only 2.8 percent of the forms had apparent errors.

Another instance of disinformation amplified by politicians happened after Colombians attending a Duque campaign rally held by former President Uribe were attacked by a swarm of bees. Congress members close to Uribe amplified an unsubstantiated claim that Petro followers were responsible for the incident—while police reports showed the bees had been disturbed by the sounds of Álvaro Uribe’s helicopter. The false claims, amplified on the social media channels of candidates and their supporters, went viral, and like in many other cases, official reports rarely reached the same audiences as those originally exposed to the disinformation.

#ElectionWatch Latin America case studies showed that content circulated along political lines in Colombia and proved those who shared or saw a false claim were rarely also exposed to verified and accurate information about the same issue on social media. Larger-scale studies confirmed this insight—a report from MOE based on an analysis of more than forty-four million social media publications about Colombian elections also concluded that “when information is refuted, it is highly unlikely that [the debunking] gets to the community that viralized it in the first place.”

### Disinformation and Misinformation Shared by Hyperpartisan Media and Blogs

False claims not only spread faster and more widely than verifications, it did so in spaces where mostly partisan content circulated. This was another consequence of the intense polarization Colombia experienced during these elections, as one-sided political pages and groups amassed large followings on social media and managed to create significant communities around them—some with more than one million fans. These digital spaces often worked as “echo chambers” for content that favored one side and attacked the other, including false and misleading claims that went largely unchecked.

There were also several hyperpartisan websites that mirrored news outlets but published content with various degrees of distortion during the elections. Some, like El Nodo or Voces.com.co, were political blogs that carelessly combined opinions and facts in their pieces, pushed a one-sided agenda outside of the standards of objective journalism, and claimed to be “independent media.” Others, like El Expediente, used some journalistic techniques but...
consistently published unbalanced and inaccurate reports, while others, like Oiga Noticias, simply spread false news. Political leaders on both sides shared these websites’ contents, and some of these outlets benefited from the existing infrastructure of Facebook political groups that gave them a sizeable audience of like-minded users. Voces.com.co, for example, became one of the most-shared sources for political content on Facebook during the campaign. Despite being less than a year old, its posts had more interactions during the electoral campaign than posts from most traditional media in Colombia.152

WhatsApp as a Vector for Disinformation

WhatsApp was a vector for the spread of information—and disinformation—during the electoral cycle in Colombia, as in Brazil. The messaging app is ubiquitous in Colombia; it is offered by all carriers on a zero-rating basis—which means data consumed on the platform does not count against overall data usage within an individual’s mobile device service plan—making it a free everyday communication tool for many Colombians. WhatsApp’s encrypted design makes gathering complete information about the content circulating on the platform very difficult. The messaging platform began working with fact-checkers and, for the first time, gave a journalism non-profit the ability to receive questions from the public during Brazil’s elections.153 Likewise, researchers like those at the University of Minas Gerais’ Monitor Do WhatsApp created tools to partially track what happens on the platform.154 However, both tools appeared after the Colombian elections and were tailored to the Brazilian ecosystem. This made any open-source analysis about disinformation during the Colombian elections necessarily incomplete.

However, working with La Silla Vacía, a news website and local partner in Colombia, #ElectionWatch Latin America results showed how disinformation and misinformation spread on WhatsApp was cross-posted to ‘open’ social media platforms by users. During the elections, La Silla Vacía ran a fact-checking service where users forwarded messages they received on WhatsApp to the newsroom.

In one example a week before the first round of the presidential elections, the outlet was sent two
messages: the mayors of two different cities were being accused of pressuring school officials to vote for a candidate. Each message had a different city and a different candidate, and one had a spelling mistake the other did not. The wording was otherwise almost identical, and neither story could be verified by La Silla Vacía journalists.

The Atlantic Council could verify that both versions of the messages were being shared on partisan political groups by influential users, and garnered significant engagement there. The extent to which WhatsApp messages and content were re-circulated on ‘open’ social media platforms is beyond the scope of the open-source methodologies and research, but anecdotal evidence suggests it was common practice. Still, Linterna Verde’s analysis of the role of WhatsApp in Colombian elections showed how these so-called “chains”—political messages that are created to be shared in groups—were often created by political campaigns and reached users through users who often volunteered on campaigns and shared the messages with their friends and families.  

Unlike what happened in other parts of the world—such as Mexico, Pakistan, Italy, or Indonesia—the research did not show that bots, or other automated inauthentic activity, played an influential role in information flows during Colombia’s elections. Some evidence of behavior consistent with bot operation were detected, including posting rates of hundreds of tweets per hour or periods of intense publication activity after months of dormant activity. However, this activity had limited influence, since it was conducted by accounts with few followers or interactions.

**Narratives**

Disinformation in Colombia spread along partisan lines—while Duque was constantly attacked for his alleged proximity to a supposedly corrupt establishment, Petro was hit by false information that portrayed him as a left-wing terrorist close the Nicolás Maduro regime in Venezuela, and as an outlier who did not conform with societal values.

The chart on page 39 shows some of the major narratives against each candidate.
La Silla Vacía: In Colombia, Fact-Checkers Got Checked

Juan Esteban Lewin, Editor-in-Chief, La Silla Vacía

IN COLOMBIA, THE STRENGTH AND spread of disinformation was not disproportionate to those in other countries. Although determining how disinformation shaped election outcomes is difficult to do with certainty, disinformation became part of political discourse and the public debate. During Colombia's 2018 elections, some politicians attacked both the media and their opponents’ arguments by accusing them of spreading “fake news.”

At the same time, political divides in Colombia shifted: the divide between left and right became starker in a country where political divides have historically not been as distinct as in the rest of Latin America. The division was exacerbated during the campaigns around the 2016 plebiscite, when Colombians were asked to vote for or against a peace agreement between the Colombian government and the Revolutionary Armed Forces of Colombia (FARC). It was in this markedly polarized campaign that disinformation took hold.

La Silla Vacía began fact-checking public discourse in 2014 through “El Detector” (The Polygraph). We saw disinformation explode in public debates around the 2016 referendum on the peace agreement—it was when false information began to circulate widely on WhatsApp and politicians and voters began sharing and amplifying these messages that fact-checking took off in Colombia.

These efforts were largely in vain. Fact-checkers debunked but did not prevent the spread of false narratives claiming, for example, that pensions would be reduced to pay monthly wages for demobilized guerrillas or that the Colombian peace agreement included “gender ideology” that would influence the sexual orientation of children.

La Silla Vacía quickly came to the conclusion that fact-checking can only help stop hoaxes when verified information is distributed by real people in whom Colombians trust.

To address this challenge, La Silla Vacía pioneered an effort to verify messages circulating on WhatsApp and to distribute verified content also through the messaging platform. We asked users to send in content they assumed was false, along with evidence that the messages had been shared within WhatsApp groups. La Silla Vacía’s commitment was to fact check these messages and send verified information back to users, while users committed to circulating debunked content back into their WhatsApp groups.

This was both a success and a failure: the effort was a success because the fact-checking initiative became very popular among users; the effort was a failure because the fact-checking team could not keep up with demand.

Disinformation continued to spread in the following months and years. During the 2018 elections, the spread of disinformation became a clear problem as the left-right divide deepened and people on both sides repeated disinformation and misinformation that reinforced their points of view.

Although La Silla Vacía simply did not have the resources necessary to repeat the WhatsApp experiment, the team fact-checked through Twitter, on television, and on our website—the pieces we published verifying information received a great deal of both attention and criticism. Perhaps that’s the future: an environment where fact-checkers are fact-checked.
Narrative | Background | Examples of False Information
--- | --- | ---
Petro, his circle, and his supporters as vandals | During his time as Bogotá mayor (2011-2015), Petro was close to political minorities and grassroots movements that some on the right identify as “vandals.” | Uribe supporters accused Petro of attacking the former president with bees; false reports of one of Petro’s sons being in debt.\(^{160}\)

Duque as the candidate of a corrupt establishment | Duque was seen as the candidate favored by powerful economic interests and Colombian political elites. | Petro supporters aired unjustified fraud claims against the National Registry; Duque was falsely accused of plotting fraud with a cousin who supposedly worked in the National Registry.

“The FARC candidate” and the Venezuela threat | After more than fifty years as an armed group, the Alternative Revolutionary Force of the Commons—the political party born after the FARC signed the peace agreement—went through their first election cycle as a legitimate party. Meanwhile, old videos showing Petro’s admiration for late Venezuelan leader Hugo Chávez surfaced. | A photoshopped image of FARC leaders wearing Petro t-shirts made the rounds on WhatsApp. The idea that electing Petro would “turn Colombia into another Venezuela” fed many memes and social media messages, some originating from Venezuela.

---

**IMPAKT ON THE ELECTIONS**

The most pressing question about the impact of disinformation and misinformation in Colombia’s elections is the extent to which they influenced voting results. This is a remarkably hard question to answer: each person’s decision about voting is affected by many different variables, making it difficult to isolate the effects of disinformation.\(^{161}\) However, four tangible effects were clear: polarization and disinformation were mutually reinforcing, disinformation had an agenda-setting effect in news coverage, media coverage of disinformation and misinformation sometimes seemed to amplify such content, and disinformation had a connection with the erosion of trust in democratic institutions.

While polarization shaped disinformation flows on social media, disinformation may also have deepened and expanded polarization. The fact that hoaxes and corrections were shared by different communities according to their political leanings—and that polarized media were able to amass big audiences in short timeframes—show that disinformation might have been instrumental in engaging people at both ends of the political spectrum and furthering divisions.

Disinformation and misinformation also shaped media coverage of the campaign, and of the candidates’ agendas. Candidates often had to correct disinformation or misinformation against them, and media reported and covered both the falsehoods and the corrections, sometimes extensively.\(^{162}\)

Finally, it is likely that news outlets played a role in amplifying some false claims through extensive coverage.\(^{163}\) An #ElectionWatch Latin America analysis showed that a viral Facebook post, using a picture of former adult film actress Mia Khalifa, claimed Petro had an illegitimate daughter who announced her support for Duque. The story was false, but some voters believed it even after most Colombian media reported this. Some stories gathered thousands of interactions on social media, as Figure 2 shows.

Another possible effect of disinformation in the Colombian election was its likely contribution to the erosion of trust in electoral institutions. Some of the biggest instances of disinformation, like the alleged electoral fraud case, were based on the premise of suspected institutional failures or corruption. The wide circulation of disinformation about electoral fraud showed the degree of distrust many Colombians felt toward their electoral authorities, and its wide diffusion also likely deepened citizens’ skepticism and confusion.

Fortunately, the E-14 episode did not compromise the integrity of the elections once the fraud claims were debunked, as Petro ended up accepting the results. But this episode shows there is a need for greater understanding by the public of the intricacies...
of the electoral system. It also shows official institutions might benefit from a more aggressive communication strategy and faster internal processes. While a rumor may be amplified significantly in a matter of minutes, an official entity often takes hours to draft, approve and publish a press release with the accurate information.

However, #ElectionWatch Latin America work, as well as other institutions’ research on disinformation in social media, undoubtedly had a positive impact on the Colombian information ecosystem. The country saw a sprout of events, reports, and projects that aimed to approach the issue from different perspectives. Linterna Verde’s work offers some encouraging evidence that Colombian social media users increasingly mistrust reports shared with them online.164

### INSTITUTIONAL REACTIONS

#### Government

This was the first election in which authorities identified disinformation as a risk and took actions to proactively counter it. While the National Registry often released corrections of false information about the election process, the Ministry of Interior produced content warning the population about disinformation more broadly. In turn, the judiciary prosecuted a landmark case, in which a video imitating the aesthetics of the Duque campaign prompted supporters to stay home and refrain from voting in the second round. The author was located by the General Attorney’s Office and asked to give a statement.

Still, government authorities had to deal with the complications of a regulation meant to balance efforts to combat disinformation with the constitutional duty of protecting democratic freedoms. Also, internal-communication processes proved slow in effectively countering hoaxes on social media. While misinformation sometimes became very popular in a matter of minutes, the process of producing, approving, and communicating an appropriate response took hours.

#### Technology and Social Media Companies

Facebook partially funded several projects that sought to tackle disinformation in the country, including #ElectionWatch Latin America, Colombia Check, La Silla Vacía and El Poder de Elegir. These partnerships were part of global efforts by the company to identify and combat disinformation and misinformation on its platform. Facebook also ran campaigns in local media aimed at teaching users how to detect and verify misinformation circulating on social media. Twitter, in turn, had contact with MOE and took part in communicating their results in a workshop in Bogotá, though the company took no part in the development or funding of MOE’s study.

Analysts have observed that Latin America and other parts of the world do not play a proportionate role in the design of technology products used in the region.

---

**TABLE 6**

<table>
<thead>
<tr>
<th>Headlines</th>
<th>Outlet</th>
<th>Total Engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td>La supuesta hija no reconocida de Gustavo Petro</td>
<td>semana.com</td>
<td>29,600</td>
</tr>
<tr>
<td>Supuesta hija no reconocida por Petro es Mia Kalifa</td>
<td>rcnradio.com</td>
<td>14,300</td>
</tr>
<tr>
<td>Mia Khalifa, la actriz porno a la que señalaron de ser la hija negada de Petro</td>
<td>semana.com</td>
<td>11,000</td>
</tr>
<tr>
<td>Petro rechaza difusión de imagen de Mia Khalifa en la que dicen que es hija suya</td>
<td>pulzo.com</td>
<td>5,900</td>
</tr>
<tr>
<td>Noticias falsas sobre Gustavo Petro: dicen que esta reconocida exactriz porno es su hija</td>
<td>pubimetro.co</td>
<td>500</td>
</tr>
</tbody>
</table>

*SOURCE: Buzzsumo.*
There is the generalized concern among Colombian observers that, for all the presence social media giants have in Latin American countries and their dialogue with local journalists and disinformation researchers, the local populations’ concerns exert very little influence on decisions by technology companies. Technology and communication platforms don’t have strategies to tackle misinformation and expedite content moderation as specific to Colombia and other Latin American countries as they do to other parts of the world.65

Fact-checking Agencies and the Media

Many media outlets in Colombia took fact-checking seriously for the first time around the 2018 presidential elections. El Tiempo and Semana, Colombia’s more influential print outlets, created dedicated fact-checking sectors or teams. Media who already focused on these techniques, such as Colombia Check or La Silla Vacía, reached a larger audience and became more influential as they made alliances with bigger and more traditional outlets.

However, disinformation was so abundant that media had a hard time deciding what to debunk. This overrode their capacity to analyze and verify rumors or false information. As a result, many false statements and stories were never corrected. And even when media debunked false content, their work did not have a proportional reach when compared to the examples of disinformation themselves, particularly not in the digital spaces where disinformation and misinformation circulated.

Civil-society Organizations and Academic Institutions

Some universities and think tanks implemented projects aimed at understanding disinformation in Colombia on a deeper level. At the university level, the production of results, however, is still a work in progress, and its diffusion has been limited to academic circles. Think tanks have similarly taken action, but—unlike universities—they have taken steps to assure the work is seen more broadly, by the public and the media. Linterna Verde authored a report about disinformation on WhatsApp and began conversations with Colombian civil society and media about the matter.66 MOE conducted a study of 44 million pieces of content on social media about the elections. While disinformation was only one of their topics, their findings reached the media.

There were many debates about disinformation organized by civil-society organizations in Colombia. The National Democratic Institute led a series of encounters and conferences with researchers and experts. In their advocacy role, MOE asked candidates to refrain from spreading false information. There were some efforts like No Como Cuento or Convivencias en Red, led by other organizations, that sought to further understand disinformation and to coordinate responses and actions. However, their efforts could benefit from better communication, as not all actors know what their peers are doing and how they can collaborate with each other. Cooperation or synergies remain, therefore, limited.

LOOKING AHEAD: COLOMBIA

As Colombia prepares for local and departmental (state-level) elections in 2019, and for presidential elections in 2022, three main concerns regarding disinformation are likely to emerge.

First, the existing infrastructure of partisan social media profiles, groups, and pages remain operational—these profiles, groups, and pages are likely to become increasingly active ahead of the elections. Such partisan actors are likely to once again drive false and misleading information about the candidates and the electoral process. In the coming years, Colombia’s independent media, public institutions, and civil-society organizations will face similar challenges to those they encountered in 2018. These stakeholders should work in collaboration to ramp up efforts to better reach audiences impacted by disinformation and to more effectively understand the content, formats, and channels necessary for bridging the gaps between where news is published and where users consume it.

Second, Colombia’s Congress is weighing decisions on several bills that seek to regulate social media, and the Constitutional Court began a public debate on the matter before ruling on a libel case pertaining to social media. In considering solutions to disinformation, Colombia faces a dilemma: To address disinformation, should the country strengthen regulations at the risk of infringing on freedom of speech, or should the country preserve existing laws that do not account for Colombia’s new information environment and that are still insufficient for prosecuting cases of illegitimate online activity? The outcome of this debate will be hugely consequential for the Colombian information ecosystem—in elections and beyond.

Finally, while automation did not play a central role in the 2018 presidential elections, other instances of coordinated social media behavior might surface in the future. From “deep fakes” (i.e., false videos featuring a person doing something they did not do or saying something they did not say) to “cyborg” accounts that feature both bot-like and human behaviors, researchers and journalists will have to prioritize the detection and understanding of new instances of such activity in the future.
## RECOMMENDATIONS

The Atlantic Council’s Adrienne Arsht Latin America Center and DFRLab propose the following recommendations for consideration by government, technology and social media companies, telecommunication companies, fact-checking organizations and the media, civil-society organizations and academic institutions, and international institutions. These suggestions aim at addressing the core, collective challenges posed by disinformation, misinformation, and automation in a rapidly changing information environment.

<table>
<thead>
<tr>
<th>Actor</th>
<th>Challenge</th>
<th>Proposed Solution</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Government</strong></td>
<td>Electoral authorities are at times unable to verify disinformation, misinformation or automation around electoral processes in a timely manner. Some claims go completely unaddressed or are addressed only after the election has taken place. This can exacerbate distrust in the voting system.</td>
<td>Electoral authorities can provide faster responses to disinformation and misinformation and be more transparent about steps being taken to investigate and address vulnerabilities.</td>
<td>Electoral authorities can more frequently communicate with journalists and fact-checkers, streamline internal communication to allow for faster response time, and publish more details about steps being taken to debunk disinformation or misinformation and fix vulnerabilities during campaign periods. This can be done in partnership with the police, media and digital influencers.</td>
</tr>
<tr>
<td></td>
<td>Law enforcement and prosecutors are, in some instances, the only actors who can verify claims that require an official investigation.</td>
<td>Law enforcement and prosecutors can be more transparent about ongoing investigations and their respective results, when doing so does not affect the legitimacy of said investigations.</td>
<td>Law enforcement and prosecutors can dedicate more resources to investigations that involve electoral disinformation and more clearly communicate findings to the public with the help of media organizations and local government officials.</td>
</tr>
<tr>
<td></td>
<td>Electoral laws in many countries prevent federal, state, and local governments from publishing some information during the electoral period. Media black-out laws also prohibit media from reporting on election-related issues. Such laws render people unable to reference an official source to verify information.</td>
<td>Government bodies, like Offices of the Attorney General in different countries, can establish more clear guidance about existing laws that prevent public institutions from publishing information in the days preceding an election and begin considering whether black-out laws could be restructured for a digital-first environment wherein voters increasingly rely on social media and the web for information during elections.</td>
<td>Government bodies, like Offices of the Attorney General in different countries, can better define and provide more clarity about which pieces of information can be published by state institutions during the electoral period. These clarifications can be published online and divulged to the public ahead of and during elections with the help of media organizations and local government officials. Media should be allowed to report on election-related disinformation up to the day of the election.</td>
</tr>
<tr>
<td>Actor</td>
<td>Challenge</td>
<td>Proposed Solution</td>
<td>How</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Government</strong> (continued)</td>
<td><strong>Electoral laws have not caught up to trends in digital information consumption. Prosecutors have a difficult time trying cases that involve digital forensics or do not have clearly outlined penalties for actors pushing disinformation or engaging in automation.</strong></td>
<td><strong>Electoral authorities, police, prosecutors, and the judiciary should examine potential updates to slander and libel laws that apply to a digitally connected world.</strong></td>
<td><strong>At the national and subnational level, governments can debate laws about transparency of ad spending online. When relevant, governments can also partner with technology and social media companies to publish reports holding political parties at all levels of government responsible for their media spending and buying, especially where it pertains to the hiring of marketing companies to send political advertisements through encrypted messaging platforms.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Disinformation and misinformation about the next cycle of local and municipal elections will soon begin to appear.</strong></td>
<td><strong>Electoral authorities can form an interdisciplinary group to discuss possible measures based on lessons learned from the national elections of 2018.</strong></td>
<td><strong>Electoral authorities can create multi-stakeholder task-forces to discuss disinformation in local elections and further train staff in cities and municipalities to recognize and verify false information in partnership with independent third parties, like civil-society organizations.</strong></td>
</tr>
<tr>
<td><strong>Technology and Social Media Companies</strong></td>
<td><strong>Barriers to entry exist on encrypted messaging platforms for journalists and researchers who wish to more effectively study and understand disinformation and how such platforms can serve as vectors for its spread during election cycles.</strong></td>
<td><strong>Encrypted messaging platforms can provide further information about how the platforms work and what actions are being taken, or could be taken, to deter the spread of disinformation.</strong></td>
<td><strong>Encrypted messaging platforms can consider sharing information that paints a picture of usage on the platform—for example, how many groups exist, how many have public links and the size of groups according to categories—to allow for the independent investigation of disinformation by fact-checkers and the media. Platforms can also consider communicating directly with its users about the threat of disinformation, for instance by providing public service announcement push notifications.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Some companies and platforms exhibit both features of one to one messaging and broadcasting. The encrypted nature of the platforms, along with broadcast features that enable messages to go viral, can open doors for the spread of disinformation that is both difficult to track and difficult to source.</strong></td>
<td><strong>Technology and social media companies, in understanding the implications for the spread of disinformation of point to point communications platforms vs. broadcast platforms, can work to adjust product features and functions to account for vulnerabilities of broadcast messages.</strong></td>
<td><strong>Encrypted messaging platforms, in better understanding the effects of the features they offer users, can adjust options to minimize broadcast features that increase the potential for disinformation to go viral with no pathways for fact-checkers and journalists to trace their spread.</strong></td>
</tr>
<tr>
<td>Actor</td>
<td>Challenge</td>
<td>Proposed Solution</td>
<td>How</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Technology and Social Media Companies</strong></td>
<td>The guidelines that govern user behavior on some technology and social media platforms are not always clear to all users, leading some groups and individuals to at times claim they are unfairly censored by technology and social media on the respective platforms.</td>
<td>Technology and social media companies can provide clearer guidelines about the rules and terms of service that apply to user behavior on their platforms.</td>
<td>Technology and social media companies can streamline and better communicate clear guidelines about their terms of service and share more information about pages and accounts that are taken down with the public to increase understanding of what constitutes inauthentic behavior. The amount of information to be shared can be weighed to account for potential security risks and risks to privacy.</td>
</tr>
<tr>
<td><strong>Technologies and Social Media Companies</strong></td>
<td>Technology and social media companies sometimes lack immediate and on-the-ground local knowledge about national or subnational political contexts and country-specific disinformation flows.</td>
<td>Technology and social media companies can establish more alliances with local institutions and civil-society organizations to better understand local challenges of disinformation.</td>
<td>Technology and social media companies can capitalize on channels of communication that were opened with third parties during the 2018 elections to deepen and expand their knowledge of on-the-ground political developments and information consumption. Companies can open or expand country offices in key markets to speed up the time it takes to address violations of terms of service.</td>
</tr>
<tr>
<td><strong>Telecommunications Companies</strong></td>
<td>Telecommunications companies’ zero-rating policies have created incentives for social media users to remain in a closed online space within platforms, rendering it difficult for them to verify claims using external resources.</td>
<td>Telecommunications companies, along with technology and social media companies, can re-examine zero-rating policies through the lens of disinformation.</td>
<td>Telecommunication companies can work with technology and social media companies and fact-checkers to discuss the possibility of including links to fact-checking websites in zero-rating policies, so users can have access to more resources when engaging with information.</td>
</tr>
<tr>
<td><strong>Fact-checking Agencies and Independent Media</strong></td>
<td>Fact-checkers have a difficult time reaching audiences most affected by disinformation or those that rely mostly on encrypted messaging platforms for news.</td>
<td>Fact-checking agencies and independent media can consider new content and formatting that better resonates with and better engages users most pre-disposed to misinformation on social media.</td>
<td>Media can experiment with new framing of content verifying disinformation to learn what is most clear and best resonates on social media. They can dedicate more time to measuring audience sentiment and reactions to these experiments to tailor messaging in the most effective way.</td>
</tr>
<tr>
<td><strong>Fact-checking Agencies</strong></td>
<td>Fact-checking organizations and the media at times amplify disinformation in their attempts to address individual cases—this can magnify the problem and exacerbate distrust.</td>
<td>Fact-checkers can better verify narratives rather than only instances of disinformation, and better target verified articles to the audiences affected by disinformation.</td>
<td>Fact-checkers can improve their use of social listening and analytics tools for a more comprehensive understanding of disinformation consumption and groups that might find value in receiving fact-checked articles.</td>
</tr>
<tr>
<td>Actor</td>
<td>Challenge</td>
<td>Proposed Solution</td>
<td>How</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fact-checking Agencies and Independent Media (continued)</td>
<td>Not all fact-checking organizations and independent media are trusted by the public.</td>
<td>Both fact-checkers and the media can work to increase transparency in reporting and methodology to bolster credibility. Independent media can also continue to adhere to the highest standards of journalistic integrity.</td>
<td>Media can ensure that all relevant parts of a debate are portrayed in articles or coverage. Stories should continue to be thoroughly sourced and fact-checked. Mistakes should be corrected and publicized in a timely manner.</td>
</tr>
<tr>
<td>Civil-society Organizations and Academic Institutions</td>
<td>Academic findings about disinformation do not always reach or inform the public debate.</td>
<td>Academic researchers can improve their outreach to media and the broader public.</td>
<td>Academia can more frequently partner with the media to publicize results of their studies and maintain direct conversations with civil-society organizations and politicians.</td>
</tr>
<tr>
<td></td>
<td>Civil society and academia, in analyzing disinformation, are at times limited in their ability to target research at the digital spaces where information is consumed in different locations.</td>
<td>Civil society and academia can continuously target research and pursue or expand upon partnerships that enable them to study user behavior where information is being consumed.</td>
<td>Civil-society and academia, in continued partnership with technology and social media companies, including encrypted messaging platforms, can work to open new doors for analyzing the information environment in the digital spaces and platforms where users are most actively consuming information.</td>
</tr>
<tr>
<td>International Organizations</td>
<td>Disinformation is often transnational in nature and can be a threat to democracies—this type of threat is not constrained by physical borders.</td>
<td>International organizations can continue to include efforts to combat disinformation as part of election monitoring initiatives and continue funding local research, advocacy, educational and media projects aimed at combating disinformation.</td>
<td>International organizations can better train election monitors to understand disinformation flows and dynamics and continue supporting cross-cutting projects to address the issue across regions.</td>
</tr>
</tbody>
</table>
Conclusion

In Latin America, a region where inequality persists and large segments of the population do not yet have enough to eat, digital engagement, especially on messaging platforms, is soaring. Around 215 million people use the Internet at least once per month from six countries in the region: Argentina, Brazil, Colombia, Mexico, Peru and Chile. Of mobile phone Internet users in Brazil, 93 percent actively use WhatsApp. Brazil and Mexico alone comprised 38 percent of WhatsApp users in 2018. This is indicative of a massive shift in information consumption.

As the region, and other corners of the world, approach ever-higher rates of connectivity, time is of the essence. Disinformation and misinformation are problems nested in broad contexts—and in trying to minimize the negative impacts of both, actors across the board will also have to assure freedoms of expression and privacy are upheld.

In Latin America’s case, where research shows organic disinformation and automation far outweighs any influence by foreign government actors, faster and more transparent multi-stakeholder action aimed at addressing false narratives will be key to combatting disinformation and misinformation in an environment of polarization. Likewise, more clarity not only on existing regulations but on attempts to solve the challenges of disinformation can amplify trust and reaffirm democratic legitimacy.

The challenges disinformation, misinformation, and automation pose to society do not exist in a silo. These challenges are also not restricted to Latin America.

As the world prepares for elections in 2019 and beyond, government, the private sector, civil-society, media and more must work collaboratively to share lessons and best practices. Disinformation, while often uniquely manifested in every country, is a borderless challenge with global repercussions. A collective approach is the only viable solution.
Acknowledgments

Just as today’s information environment transcends borders, so too did the efforts to combat disinformation and to strengthen digital resilience as part of #ElectionWatch Latin America. This initiative included a host of actors, from civil society, to media, to electoral authorities, to the private sector from the United States, Europe and Latin America.

For their partnership and support, the Atlantic Council’s Digital Forensic Research Lab (DFRLab) and Adrienne Arsht Latin America Center would like to acknowledge the contributions of the many stakeholders and in-country partners that helped make this publication a reality.

In Brazil, a special thank you to our partners Fundação Getulio Vargas’ Department of Public Policy Analysis (FGV-DAPP) and Jornal O Globo, specifically the “Fato ou Fake” team. In Colombia, thank you to our partners La Silla Vacía, Linterna Verde, and Centro Gabo. In Mexico, our gratitude goes out to our partners Animal Político and Verificado 2018.

Thank you also to the many stakeholders who provided their insight and feedback through consultations: The Organization of American States; in Mexico, the Instituto Nacional Electoral; in Brazil, the Instituto Tecnologia & Equidade, ITS Rio, Internet Lab, the Universidade Federal de Minas Gerais, the Universidade Federal do Rio de Janeiro’s Media Lab, and others; in Colombia, Chicas Poderosas, and many more.

The Atlantic Council would also like to recognize Juan Felipe Celia, whose leadership at the inception of this project paved the way for the efforts laid out in this report. Thank you to Paula García Tufró and Nicholas Yap for their efforts and support, as well as to Ben Nimmo, Fernando Meneses, Iain Robertson and the editors that contributed to this publication. A special thank you to Roberta Braga and María Fernanda Pérez Argüello for their leadership and management of this paper.

Finally, the Atlantic Council extends a heartfelt thank you to Open Society Foundations (OSF), whose support of the Atlantic Council’s #ElectionWatch Latin America work made possible this comprehensive effort to strengthen digital resilience in Latin America and beyond. The work continues!
Glossary of Key Terms

**Automated traffic**—social-media traffic primarily driven by automated accounts, like botnets (see definition below).

**Bot**—a social media account that has been automated to carry out certain actions, typically liking, sharing, reposting, or following other users. Bots do not usually engage other users in conversation. Bots can be further broken down into commercial, political, and spam bots.

**Commercial bot**—a bot whose activity can be rented out to anyone willing to pay for likes or reposts. Commercial bots are usually apolitical, and often repost or like content on a wide range of unrelated subjects, and in many languages.

**Political bot**—a bot created to amplify one particular political message or stance. Political bots usually post on one subject, often at a high rate.

**Botnet**—a group of bots organized by the same person or algorithm, so they behave in the same way at the same time. Botnets can consist of hundreds of thousands of accounts, although these are becoming increasingly rare.

**Coordinated inauthentic behavior (CIB)**—online behavior intended to deceive audiences about its authors or motives, conducted by a number of users in coordination with one another. CIB is banned on Facebook, and was the reason used for removing a number of Russian and Iranian disinformation assets.

**Coordinated online network**—a group of online users, web pages, social media, or Internet forum accounts, organized by the same idea, organization, or person. Members of a network push out the same narrative, or narratives; have similar behavior patterns; often endorse each other and share the same content, sometimes at different times. Sometimes, but not always, the creation date of accounts is the same.

**Disinformation**—false information spread with intent to deceive. To prove that a particular incident counts as disinformation, it is necessary to prove both that the information was false and that the source spread it deliberately.

**Election manipulation**—an attempt to influence the outcome of an election through covert, undeclared, or illegal means, or by disinformation. Election manipulation can be domestic or foreign in origin. It is distinguished from electioneering by the use of covert, undeclared, or illegal means, and by the use of disinformation.

**Fake news**—this term has become so debased that it can no longer be assigned a definition.

**Foreign interference**—an attempt to adversely affect, or undermine confidence in, any political, governmental, or democratic process, or prevent the exercise of human or democratic rights, through coercion, corruption, or the use of covert, malicious, or deceptive means, acting from abroad.

**Inauthentic behavior**—behavior on social media that is conducted for a reason other than the apparent one. Examples of inauthentic behavior include selling likes, following other accounts for pay, and setting up anonymous accounts to covertly promote other organizations.

**Like farm**—an organization that uses a substantial number of social media accounts to sell likes, reposts, and follows to real users who want to make themselves look more important. Like farms are typically commercial, but the return is low: a like farm exposed in 2018 by DFRLab sold ten thousand likes on Instagram. Like farms can use automated accounts, human users, or any combination of the two.
Media outlet—not all media outlets subscribe to the same standards. They can be classified in the following ways:

Alternative media outlet—a media outlet that contrasts itself to mainstream media and offers its readers an “alternative” take on events and processes. This is one of the most common ways in which disinformation actors attempt to win an audience.

Commercial media outlet—a media outlet whose primary goal is to earn money for its shareholders. It may or may not show independence.

Fringe media outlet—a media outlet that does not have the qualities of the mainstream media. This divergence from the mainstream may lie in the size of its distribution and following, or its adherence to journalistic standards, or it may flow from a self-declared opposition to the “mainstream media” or “MSM.” Such outlets may or may not share conspiracy theories or aggregate and amplify other media outlets—including mainstream media, other fringe media, and blogs.

Independent media outlet—a media outlet that retains editorial independence, regardless of its source of funding.

Public broadcaster—a media outlet that receives public funding but retains editorial independence from a government or political party.

State-backed media outlet—a media outlet that is partly owned by the government or is owned by a state-owned company.

State-owned media outlet—a media outlet that is overtly or covertly funded by the government.

Misinformation—false information spread with intent that cannot be ascertained, or which can be shown not to be deliberate (e.g., if the source subsequently corrected itself).

Organic content—content generated by human users.

Organic traffic—social media traffic that appears to be primarily generated by spontaneous users, rather than a coordinated campaign. (Given the nature of online conversations, even organic traffic is likely to have some automated component—for example, by advertising bots picking up a popular hashtag to increase users’ awareness of the product being promoted.)

Troll—a human being who systematically posts inflammatory, divisive, hyperpartisan, or abusive content, often under cover of anonymity. The word “troll” is not a measure of attribution, but describes the behavior of an individual user.

Troll farm/factory—an organization that employs a substantial number of trolls, usually to promote a political stance or attack its opponents. Troll operations can be located in a single website or a number of websites, or organized remotely.
About the Authors

Roberta Braga, Associate Director, Adrienne Arsht Latin America Center, Atlantic Council
Roberta Braga is an associate director at the Atlantic Council’s Adrienne Arsht Latin America Center, where she leads projects on Brazil, disinformation and misinformation in elections, trade and commerce, and energy in Latin America. In partnership with the Council’s Digital Forensic Research Lab (DFRLab), Roberta has for the past year and a half managed the Center’s #ElectionWatch Latin America project focused on exposing disinformation around elections in Brazil, Mexico, and Colombia. Braga previously worked as a strategic communications analyst at the US Department of Homeland Security, and as a corporate affairs and public relations specialist at Promega Corporation, an international biotechnology firm headquartered in Madison, Wisconsin. She has been quoted in The New York Times, The Wall Street Journal, The Financial Times, Axios, Brazil’s O Globo and Folha de S.Paulo. Originally from Brazil, Braga is a native Portuguese- and English-speaker, and fluent in Spanish. She has a master’s degree in global communication and public diplomacy from the George Washington University’s Elliott School of International Affairs.

Luiza Bandeira, Digital Research Assistant, Digital Forensic Research Lab (DFRLab), Atlantic Council
Luiza Bandeira is a digital research assistant and the lead researcher on Brazil at the Atlantic Council’s Digital Forensic Research Lab (DFRLab), a hub of analysts tracking events in governance, technology, security, and where each intersect. As part of the #ElectionWatch Latin America project in Brazil, Bandeira identified, exposed and explained cases of disinformation around the country’s consequential 2018 elections, where she also monitored the spread of disinformation on WhatsApp in conjunction with the Latin America-based group Chicas Poderosas. A multi-media journalist with over ten years of experience covering elections, political reforms and economics, Bandeira has written about foreign affairs and technology for the BBC World Service and for Brazil’s leading newspaper Folha de S.Paulo. Luiza Bandeira has a master’s degree in social policy and development from the London School of Economics and has worked as a researcher for the Harvard Business School’s Latin America program.

Jose Luis Peñarredonda, Digital Research Assistant, Digital Forensic Research Lab (DFRLab), Atlantic Council
Jose Luis Peñarredonda is a digital researcher and journalist based in Bogotá, Colombia. His main area of interest is the intersection of technology, politics and culture. He is a digital research assistant at the Atlantic Council’s Digital Forensic Research Lab. In the past, he has worked with civil society institutions like Tactical Tech, Fundación Karisma and the Gabriel García Marquez Foundation. His journalism has been published on the BBC, NPR, and several Latin American media outlets. He has a master’s degree in digital culture and society from King’s College London.

Maria Fernanda Pérez Argüello, Associate Director, Adrienne Arsht Latin America Center, Atlantic Council
Maria Fernanda Pérez Argüello is associate director at the Atlantic Council’s Adrienne Arsht Latin America Center, where she leads the Center’s work on Mexico, USMCA, and Central America, and contributes to projects on China- Latin America, regional trade integration as well as disinformation in Latin America. During her time at the Council, she has co-led the Center’s Central America Task Force, managed the Center’s trade portfolio, and programmed events in Asia for US policymakers. She speaks native Spanish, English, and French, fluent Italian, and near-fluent Portuguese. Originally from Costa Rica, Maria Fernanda earned a degree in European Studies from Sorbonne University in France, as well as a master’s degree in Latin American studies and political economy from Georgetown University’s School of Foreign Service. She has a master’s in international law and human rights from the United Nations University for Peace.

Donara Barojan, Assistant Director for Research and Development, Digital Forensic Research Lab (DFRLab), Atlantic Council
Donara Barojan is an assistant director for research and development at the Atlantic Council’s Digital Forensic Research Lab. She is based at the NATO StratCom Center of Excellence in Riga, Latvia. At the DFRLab, Donara analyses online disinformation campaigns around the world with a special focus on disinformation targeting elections. She also leads efforts to develop tools to monitor and counter disinformation online. Barojan’s research has been featured by numerous media outlets, including The New York Times, Reuters, the Economist, The Hill, ProPublica and Business Insider. Donara is a graduate of the London School of Economics and Political Science.
Endnotes


54


84 Fiscalia Especializada para Atención de Delitos Electorales (FEPADE), http://www.fepade.gob.mx/.

85 USMCA was not signed by the government of Enrique Peña Nieto until November 2018.


The Electoral Process and Political Dynamics - Mexico, US

Andrea Rodriguez, “Ahead of Mexico’s presidential election, Ben Nimmo and Donara Barojan, #ElectionWatch: Russian
David Alire Garcia and Noe Torres, “Russia meddling in
McMaster: US has seen signs of Russian ‘subversion and
Donara Barojan, #ElectionWatch: RT y Sputnik
Donara Barojan, #ElectionWatch: Down Ballot Bots in
Fernando Peinado, “El mercado global de los ‘me gusta’
Sobre el INE,” Instituto Nacional Elector
“Qué es Verificado?” Verificado, 2018,
For a taxonomy of bots, see Ben Nimmo, #BotSpot:


“¿Esto es cómo mexicanos spend their day on WhatsApp,” The Mazatlan Post, February 20, 2019.


See, for instance, the initiatives No Como Cuento, (http://elavisperomov.org/nocomocuento) a media literacy initiative by journalists and civil society organizations; or Centro Gabo’s Convivencias en Red. (https://centrogabo.org/proyectos/convivencias-en-red). an initiative aimed at understanding and tackling disinformation and fostering best practices for social media use in Colombia (a DFRLab’s local partner).


Verjel Torrado and Julián José, “Plebiscito por la paz en Colombia, una disputa más allá del contenido de los acuerdos,” Marco: Revista de Marketing y Comunicación Política, 3 (2017), 57–76.


Nicolás Galvis Ramírez, Omar David Baracaldo Orjuela, Miguel García Sánchez, and Catalina Barragán Lizarraga, “Bardometro de las Américas Colombia, Observatorio de la Democracia, Universidad de los Andes, 55


140 José Luis Peñarredonda, The Influence Industry: Personal Data in Colombia’s 2018 Legislative and Presidential Elections (Berlin, 2018).


143 Fabián Hernández, personal conversation with the author (2019).


146 Carlos Cortés and José Luis Peñarredonda, Politics (On WhatsApp) Is Dynamic: Disinformation and the spread of political “chains” in Colombia (Bogota, 2018).


155 Carlos Cortés and José Luis Peñarredonda, Politics (On WhatsApp) Is Dynamic: Disinformation and the spread of political “chains” in Colombia (Bogota, 2018).


163 Carlos Cortés and José Luis Peñarredonda, Politics (On WhatsApp) Is Dynamic: Disinformation and the spread of political “chains” in Colombia (Bogota, 2018).

164 Carlos Cortés, personal conversation (2019).


Atlantic Council Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

CHAIRMAN EMERITUS
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*Virginia A. Mulberger
*W. DeVier Pierson
*John J. Studzinski

TREASURER
*George Lund

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
*Peter Ackerman
Timothy D. Adams
Bertrand-Marc Allen
*Michael Andersson
David D. Aufhauser
Matthew C. Bernstein
*Rafic A. Bizri
Dennis C. Blair
Thomas L. Blair
Philip M. Breedlove
Reuben E. Brigety II
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
Nelson W. Cunningham
Ivo H. Daalder
*Ankit N. Desai
*Paula J. Dobriansky
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Ronald M. Freeman
Courtney Gedulig
Robert S. Gelbard
Gianni Di Giovannini
Thomas H. Glover
Murathan Günsal
John B. Goodman
*Sherri W. Goodman
*Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Brian C. McK. Henderson
Annette Heuser
Amos Hochstein
*Karl V. Hopkins
Robert D. Hormats
*Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Reuben Jeffery, III
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Sean Kevelighan
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Richard L. Lawson
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Wendy W. Makins
Zaza Mamulaishvili
Mian M. Mansha
Chris Marlin
Gerardo Mato
Timothy McBride
John M. McHugh
H.R. McMaster
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
Susan Molinari
Michael J. Morell
Richard Morningstar
Edward J. Newberry
Thomas R. Nides
Franco Nuschez
Joseph S. Nye
Hilda Ochoa-Brillembourg
Ahmet M. Oren
Sally A. Painter
*Ana I. Palacio
Carlos Pascual
Alain Pellegrini
David H. Petraeus
Thomas R. Pickering
Daniel B. Poneman
Dina H. Powell
Robert Rangel
Thomas J. Ridge
Michael J. Rogers
Charles O. Rossotti
Robert O. Rowland
Harry Sachinis
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
Richard J.A. Steele
Paula Stern
Robert J. Stevens
Mary Streett
Ellen O. Tauscher
Nathan D. Tibbits
Frances M. Townsend
Clyde C. Tuggle
Mellane Verveer
Charles F. Wald
Michael F. Walsh
Geir Westgaard
Maciej Witucki
Neal S. Wolin
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Harold Brown
Ashton B. Carter
Robert M. Gates
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teitlseh
John W. Warner
William H. Webster

*Executive Committee Members

List as of January 1, 2019
The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 778-4952
www.AtlanticCouncil.org