

**SIPA Capstone**  
Assessing Social Media-Driven  
Influence Operations in Latin America

**Client**

FireEye

**Advisor**

Neal Pollard

**Team**

Timothy Lehey

Daniel O'Quinn

Edward Shim

Jonathan Song

Fan Zhang

## **Acknowledgements.**

The Columbia SIPA Capstone team would like to extend its gratitude to any individuals or organizations that contributed to the Capstone project and assisted in advancing our research.

Professor Neal Pollard, Adjunct Professor of International and Public Affairs, whose advising and mentoring was critical to the overall success of the Capstone project.

Luke McNamara and the rest of the FireEye team, who were always available to answer our questions and provide feedback.

Suzanne Hollman and Saleha Awal for their logistical support and backing for unique opportunities that presented themselves along the way.

United States Southern Command and Special Operations Command South for taking an interest in our research and making its personnel available for consultation.

All the interviewees that provided their expertise and participated in our project. Your input was instrumental in advancing our research.<sup>1</sup>

---

<sup>1</sup> Any views expressed herein are the authors' own and do not necessarily represent those of SIPA.

## Executive Summary

Given the recent rise and influence of social media in Latin America (LA), social media (SM) has become the platform of choice for actors seeking to influence public opinion and, in effect, the electoral process. With social media-driven influence of the 2016 U.S. Presidential election dominating headlines and with six Latin American (LA) national elections in 2018, there is concern that SMDIO may impact elections. “Social media” in LA encompasses platforms such as Facebook, Twitter, WhatsApp, Instagram, and related messaging platforms. This report examines the impact of social media-driven information operations (SMDIO) on three countries with upcoming elections: Mexico, Brazil, and Colombia (MBC).

### **Key Findings**

1. SMDIO has gained significant traction over the past decade due largely to a rise in Internet access and, consequently, SM users in MBC. It is not a new phenomenon; SMDIO significantly impacted previous elections in MBC and continues to evolve in reach, scope, and creativity.
2. Generally, the majority of SMDIO campaigns are non-attributable. However, notable exceptions to this are the SMDIO campaigns by Colombian Andres Sepulveda, cyber “troll” or bullying groups, and alleged foreign nations with an interest in the political affairs of MBC. The domestic actors who employ these means are primarily political parties and candidates themselves (who debate the ethics of SMDIO in public while likely leveraging it for themselves) as well as organized crime. Moreover, there exists a burgeoning market in MBC where SMDIO is sold to the highest bidder and the allure of quick profit often outweighs social or moral implications.
3. The governments of MBC have acknowledged the existence and rapid proliferation of SMDIO over the past decade. However, rhetoric and efforts related to countering SMDIO have not deterred the visible growth of a “hacker market” and related SMDIO. While there is increased acknowledgment and discussion within both government and civil society, notably the robust government response by Brazil to counter fake news, the reality of SMDIO is that it remains a largely unregulated “wild west.”
4. What defines a SMDIO “threat” is ultimately subjective and depends on one pivotal question: according to whom? Depending where on the political spectrum one stands, one will view information through either a receptive or hostile lens and could view IO as beneficial to their cause as opposed to a “threat.” For the purposes of this report, we have assessed SMDIO from the perspective of those most invested in the integrity of the electoral process: the electorate.
5. The strategic outlook for SMDIO in MBC is bleak and does not have a simple solution. The primary challenges are: (1) everyone connected to SM is now an influencer, (2) developments in information technology continue to far outpace security considerations, (3) it is impossible to objectively quantify the impact of SMDIO on elections, and (4) it is impossible to unequivocally state the intent of SM actors, (5) responses (apologies and retractions) to fake news as the “second mover” are not as effective in affecting public opinion, and (6) it is difficult to prosecute or define an SMDIO “offense” without infringing on civil liberties or free speech.
6. Based on the current SM landscape of MBC, there is a high likelihood that SMDIO will impact the upcoming and future electoral processes as a persistent threat. There is no incentive for public or private entities to refrain from SMDIO. Moreover, the prospect of quick profit makes SMDIO commonplace. MBC must hold SM and companies accountable if the goal is to combat adverse SMDIO. At present, SM platforms such as Facebook are under increased scrutiny in the West to operate more transparently and to take proactive measures against SMDIO. In addition, public awareness and education must continue to grow if it is to match the disinformation efforts of influential actors in the SM landscape.

### Defining the “Threat”

#### **Characteristics → Context/Capabilities + Intent**

Defining a “threat” is not a binary proposition but a spectrum with fluid characteristics. **A potential social media-driven “threat” in the context of elections is identified by Characteristics, defined by Capabilities (reach), and validated by Likely Intent. Once a potential threat is identified, we measure Threat Severity using the latter two categories.**

**Identification:** We define potentially threatening SMDIO *actions* (and the actors who perpetrate them as potential threats) based on the following four criteria:

1. **Spreads disinformation** and/or factually incorrect information through SM
2. **Exerts undue or uninvited influence** on public opinion through SM i.e. Cambridge Analytica
3. **Intimidates** SM users through threat of violence, retaliation, and similar means
4. **Coerces** SM users through use of bribery, false promises, *quid pro quo*, or similar means

**Definition:** The differing societal context in which SMDIO campaigns take place and their **capabilities (reach)** are what define them as “threats.” The societal context of this report are the upcoming elections in MBC. Social Media platforms provide four key **capabilities**:

1. **Access** to targets and tools (**Reach**)
2. **Freedom of Movement** to/from targets
3. **Inadequate Deterrents**, surveillance, or legal infrastructure
4. **Belief** that one can evade consequences

In the case of SM, these capabilities are taken to an unparalleled level. SMDIO threats now have instantaneous reach to and from targets with little to no deterrence measures in place. From a cyber defense planning perspective, strategy that focuses on weakening one of these capabilities may weaken the others.

**Validation:** Threats are validated by **Likely Intent**. For example, an actor may spread a false news story (identifying characteristic) unrelated to elections on social media (capability). If the news story does not aim to impact a candidate or the electorate (lack of context) then it would qualify as a LOW or LOW-MODERATE threat in the context of elections.

#### **Threat Severity Spectrum Methodology: Capabilities (Reach) + Intent**

We categorize SMDIO threats with **LOW**, **MODERATE**, or **HIGH SEVERITY** using the following methodology specific to MBC elections. Threats may also fall somewhere between the spectrum. For example, a threat may be L-M (LOW-MODERATE) or M-H (MODERATE-HIGH).

**LOW SEVERITY (LS):** An LS threat is defined by low SM capabilities (reach) and unlikely intent to conduct threatening (as defined above) SMDIO impacting elections. An example of this would be

the majority of the electorate who may not have wide reach on SM nor the intent to subvert the electoral process.

**LOW-MODERATE SEVERITY (L-M):** An L-M threat is defined by LOW likely intent and MODERATE capabilities/reach. An example of this would be civil society organizations such as NGOs.

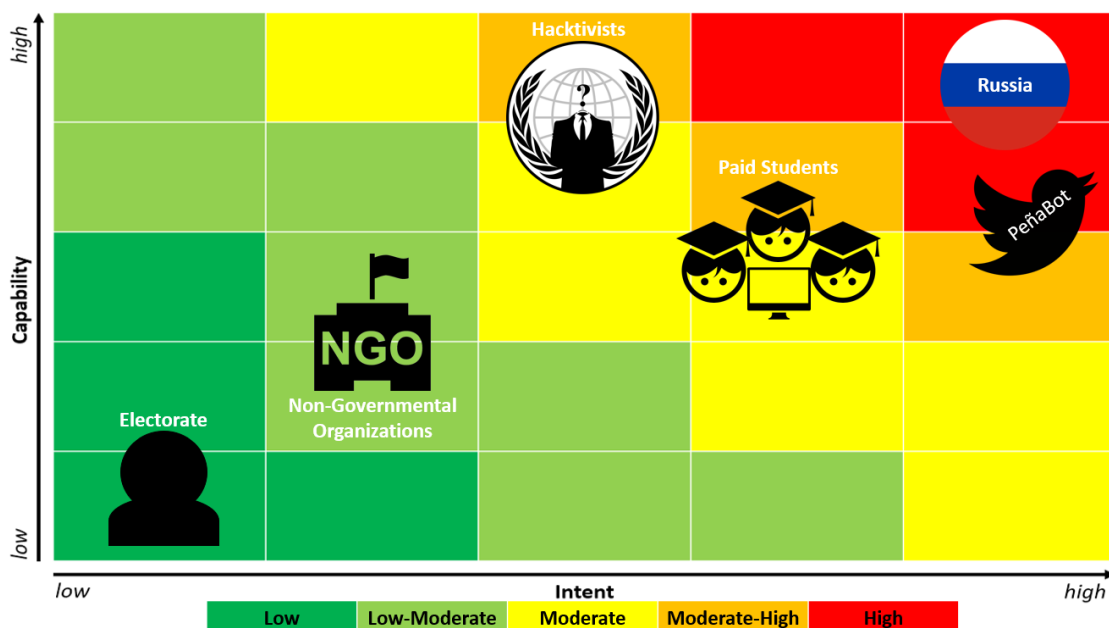
**MODERATE SEVERITY (MS):** An MS threat is defined by:

- (1) HIGH capability/reach but LOW likely intent. An example of this would be public figures such as celebrities who have massive SM reach but may not have likely intent.
- (2) HIGH likely intent but LOW capability/reach. An example of this would be disgruntled voters or foreign actors invested in election outcomes but with LOW technical capabilities/reach.
- (3) MODERATE capability/reach and UNCERTAIN intent. An example of this would be less advanced hackers and private actors such as students seeking extra income through SMDIO.

**MODERATE-HIGH SEVERITY (M-H):** An M-H threat is defined by:

- (1) HIGH capabilities/reach and UNCERTAIN intent. An example of this would be troll/cyber bullying groups and organized crime.
- (2) HIGH likely intent and LOW or LOW-MODERATE capabilities/reach. An example of this would be extremists on SM or single-issue political groups.

**HIGH SEVERITY (HS):** An HS threat is defined by advanced (HIGH) capabilities/reach and HIGH likely intent to influence the electoral process. Examples of this would be alleged actors such as Russia, Cambridge Analytica, the “Peñabots”, and high-profile hackers such as Andres Sepulveda.



### Challenges Inherent to the SMDIO Landscape

There are **challenges** unique to the SMDIO landscape that make deterrence and defense exceedingly difficult:

1. **Scope:** The SMDIO landscape includes any and every person with a device connected to SM. Effectively, *everyone on SM is an influencer*.
2. **Pace of Development:** Given the meteoric rise of social media in MBC, the evolution of SMDIO threats outpaces the ability of stakeholders to respond.
3. **Quantifying the Impact of IO:** At present, there is no viable method to quantify the impact of SMDIO on elections.

### Complicity of SM Platforms (Facebook, Twitter, WhatsApp, etc.)

While Facebook and Twitter have verbally pledged to fight misinformation, including the creation of fake accounts and use of bots, the reality is that their corporate share price is tied to number of users. This conflict of interest has resulted in limited compromise in the policy arena with mixed results in reality.

In late 2017, Twitter renewed its bot-detection app and deactivated more than 220,000 accounts that were sending out over 2.2 billion “low-quality” tweets. However, this statistic does not reveal the accounts’ country of origin. In February 2018, Facebook signed a cooperation memorandum with the Mexican National Electoral Institute (NEI) to help train government employees in “how to use Facebook.”<sup>i</sup> However, such policy efforts do not educate the public at-large nor deter the temptation for actors seeking quick profit to engage in SMDIO.

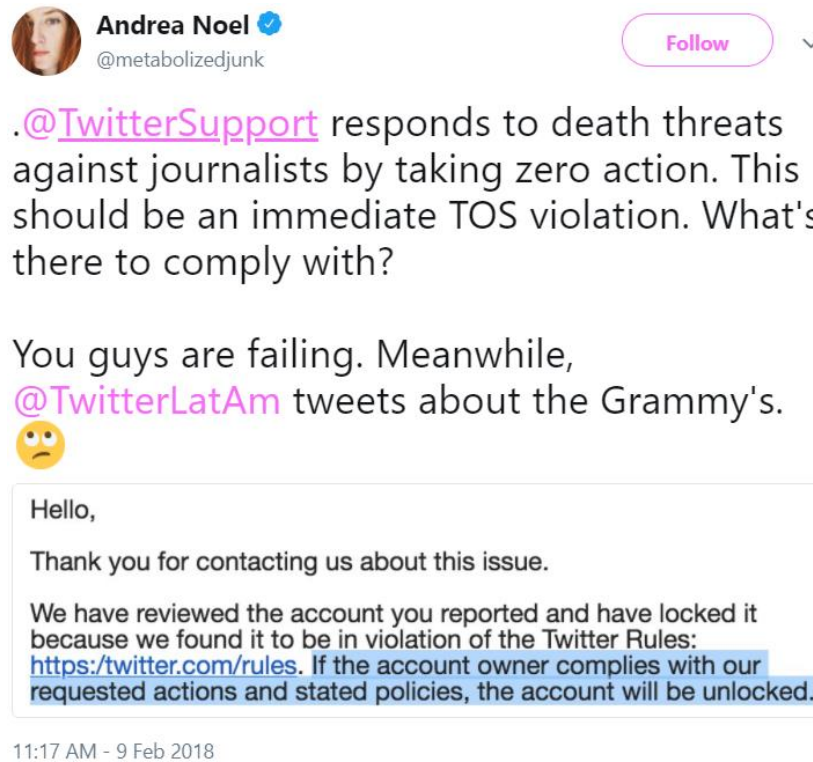
In addition, SM platforms have had lukewarm responses to violations of terms of use. Andalusia Knoll Soloff, a writer for Vice Magazine, reports that:

On March 8, 2016, freelance journalist Andrea Noel tweeted a surveillance video of a man who sexually assaulted her while she was walking down the street in Mexico City. Noel tweeted the video with the message “women should be able to walk safely” and requested that people help identify her attacker. Her timeline was immediately flooded with threats from both bots and trolls that included both her location and photos of armed men. LoQueSigue [prominent blog run by journalist Alberto Escorcia] published data clouds showing at least 20,000 mentions of Noel’s Twitter account in just one day. Many of the accounts had few followers, no photos, and failed to maintain their conversations like a real person would—all prime indicators that the accounts were operated by bots.<sup>ii</sup>

Furthermore, Noel points out that:

You see that Twitter has suspended—for life—the accounts of Milo Yiannopoulos or Azealia Banks, but they don’t focus on Latin America. I have reported dozens of accounts that have sent me death threats, and nothing has happened.

The following tweet by Noel from February 2018 is illustrative of Twitter’s response:<sup>iii</sup>



*Tweet by Noel from Feb 2018 illustrating Twitter's response to ToS violations*

Per official Twitter policy:

We believe in freedom of expression and open dialogue, but that means little as an underlying philosophy if voices are silenced because people are afraid to speak up. In order to ensure that people feel safe expressing diverse opinions and beliefs, we prohibit behavior that crosses the line into abuse, including behavior that harasses, intimidates, or uses fear to silence another user’s voice.<sup>iv</sup>

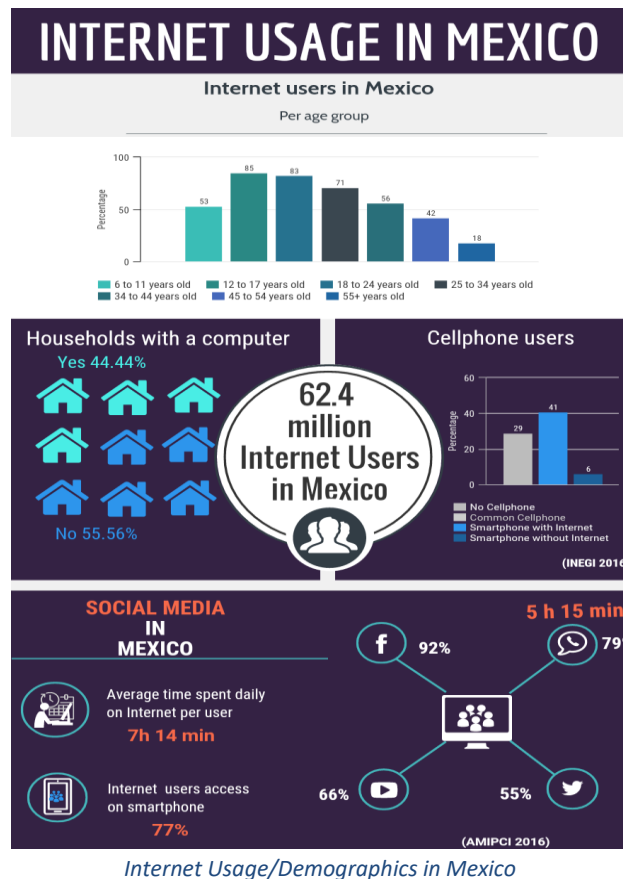
In April 2018, a network of supposed “news” sites began appearing. These sites were staunchly anti-AMLO and spread disinformation such as “AMLO is very ill” (in reference to his health) and alluded to Mexico becoming a totalitarian state similar to Venezuela under Chavez should AMLO win via Facebook and Twitter.<sup>v</sup> In response to this massive disinformation campaign, a Facebook representative stated that, “all the sites comply with the company’s policies” but declined to disclose whether the sites pay Facebook to promote their content in users’ news feeds, but says Facebook would allow them to do so.<sup>vi</sup>

Despite the fact that actors leveraging SMDIO violate platforms’ terms of use, they are continuing to weaponize it. Therefore, strategy regarding the mitigation of SMDIO must acknowledge the complicity of the platforms upon which such threats operate.

## Case Study: SMDIO in Mexican Elections

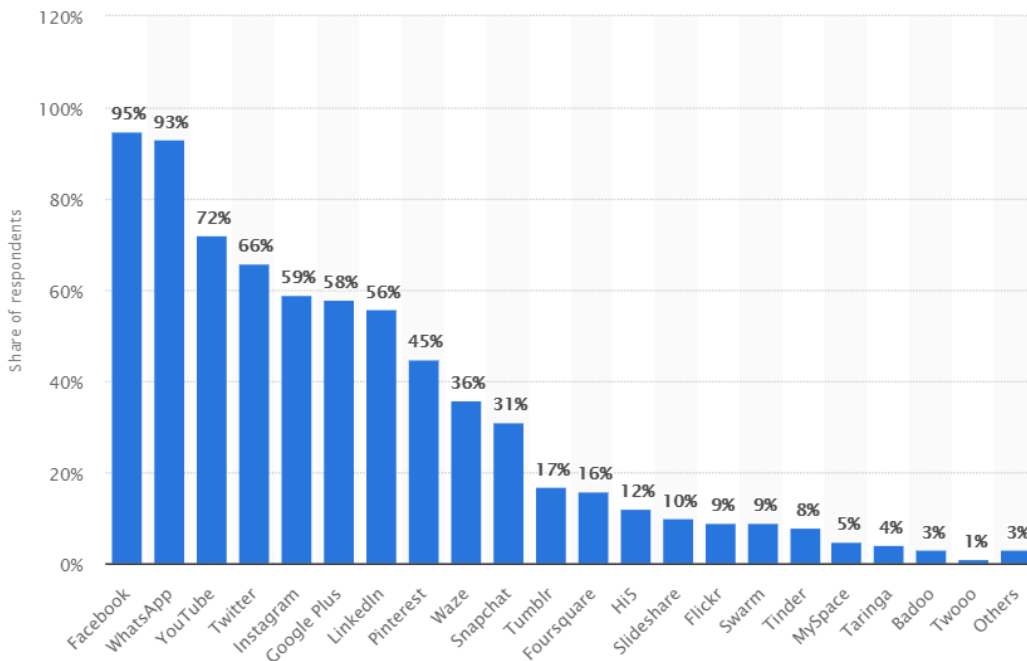
### Context

As a strategic and economic hub of Latin America (LA) that connects the region to the United States, Mexico has rapidly become a prime target for SMDIO over the past decade. Mexico's Internet use increased from 5% (approximately 5 million users) in 2000 to 41% (50 million users) in 2014. Moreover, there are 77.7 million people who use mobile telephones and two out of three have a smartphone. According to Mexico's Census Bureau INEGI, there are 62.4 million Internet users which account for a total of 57.4% of the population.<sup>vii</sup> Additionally, 73.6% of those who use the Internet in Mexico are between the ages of 6 to 34 years old.<sup>viii</sup>



Given these trends, Mexico has become an ideal target for cyber actors seeking to influence elections through SMDIO targeted at demographics active on the Internet. The following exhibit is the top ten SM platforms in Mexico as of April 2017:<sup>ix</sup>





*Top 10 SM Platforms in Mexico (April 2017)*

### **Perceptions of SMDIO**

Strategically, Mexico perceives the cyber threat in terms of impact on Critical National Infrastructure (CNI) and critical revenue generating industries such as oil and energy. However, what is less clear is the extent (or incentive) with which the national government believes that counteracting SMDIO is in its best interest. Even though Mexico has been subject to SMDIO since at least 2012, perceptions of “information warfare” are not at the forefront of policy (although it is often alluded to in public discussion) despite their influence on the electoral process. This is primarily because parties themselves have the most to gain from SMDIO. At present however, the issue of fake news is taking hold in media and civil society.

With increased internet penetration in the past decade, public users in Mexico now have an unprecedented level of access to SM. However, public capabilities to defend against SMDIO appear limited to specialists who have the technical skills to recognize and expose threats. Prominent examples include journalists such as Alberto Escorcia, hacktivists, Anonymous Mexico, civil society, and others.

In private industry, cybersecurity considerations have risen to the forefront of security planning. In Latin America, Mexico ranks second after Brazil in number of attacks against private industry but many companies do not report incidents for fear of damaging their reputations. According to PwC Mexico, 91% of Mexican companies have prioritized cybersecurity in their organizations and Mexico has the most investment in cybersecurity in Latin America as of 2015.<sup>x</sup>

### **Recent History of IO in Mexico**

A recent example of SMDIO is the 2012 Presidential Election. In 2016, Colombian hacker Andres Sepulveda stated that he hacked, spied, and manipulated social media for President Enrique Peña Nieto’s campaign. Under the direction of Miami-based political consultant Juan Jose Rendon,

whom Miami print media labeled “the Karl Rove of Latin America,” Sepulveda leveraged social media to an unprecedented scale to influence elections in LA.<sup>xi</sup> According to Sepulveda, Rendón realized that hackers could be integrated into a political operation, running attack ads, defaming the opposition, and finding ways to suppress or reduce a foe’s turnout. Sepulveda realized that voters trusted what they thought were spontaneous expressions of real people on social media more than they did experts. In his own words, “When I realized that people believe what the Internet says more than reality, I discovered that I had the power to make people believe almost anything.”<sup>xii</sup>

## **Current SMDIO: Realities of the Threat Landscape**

### **Trolls, Foreign Nations, and Political Parties**

With the imprisonment of high-profile actors such as Sepulveda, potential threats who could conduct SMDIO include “troll” or cyber bullying groups such as Legion Holk and SDLG (Seguidores de la Grasa). In the past, they have conducted Facebook and Twitter attacks on prominent journalists and against political movements. Moreover, foreign nations and political parties seeking to gain an advantage have already begun leveraging SMDIO. These include hiring hackers on the open market and political data analysis firms such as Cambridge Analytica.<sup>xiii</sup>

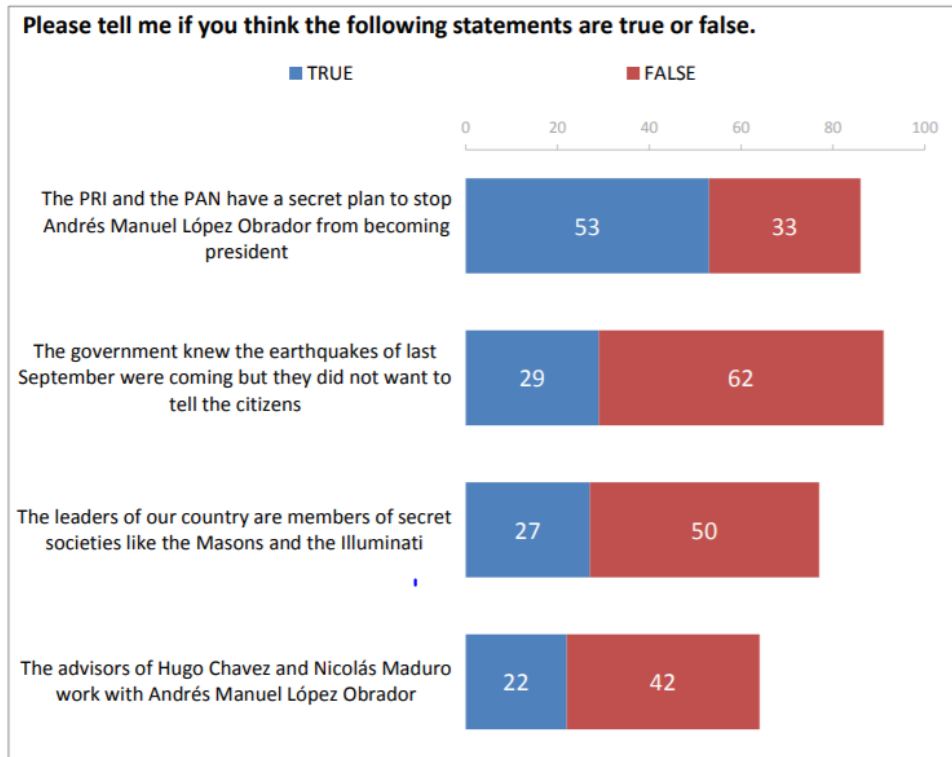
Former U.S. National Security Advisor H.R. McMaster believes that Russia is already conducting IO impacting the Mexican elections.<sup>xivxv</sup> If the most recent U.S. election is any indication, noticeable patterns of actors in Russia purchasing Mexican political ads at scale or posting on Facebook in an observable bot-like pattern would corroborate this claim.<sup>xvi</sup> Russian television network RT is also connected to the Mexican Presidential elections, as frequent RT en Espanol contributor John Ackerman is married to Irma Sandoval. Sandoval is part of leftist candidate Andres Manuel Lopez Obrador’s (AMLO) campaign team and, according to news outlet El Pais, has been promised a position in his cabinet if he wins.<sup>xvii</sup>

According to Mexican news publication El Pais, as of March 2018 political parties are using bots and trolls at a rate unseen to date in the country.<sup>xviii</sup> Furthermore, according to former trolls, an increasing practice by political parties is to leverage fake news websites, paid influencers, identity theft, and online harassment to influence voters. While parties deny SMDIO, consulting firm Metrics Mexico determined that over 18% of Twitter content in Mexico for the month of March 2018 was created by bots and paid influencers.<sup>xix</sup>

### **Attitudes towards SM in Mexico**

According to Noel, Mexicans view misinformation and social media manipulation as the norm because they have never seen “a clean Twitter environment.”<sup>xx</sup> In addition, a Wilson Center study conducted in April 2018 discovered that a significant number of Mexicans are still susceptible to fake news regardless of the medium.<sup>xxi</sup> The poll results below illustrate Mexican citizens responses to a series of fake statements:

**Figure 1. Share of people that believe in a series of fake statements**



*Over 50% of Mexicans believe the PRI/PAN are conspiring against AMLO and nearly 30% believe the government knew in advance about the earthquake.*

As a result, social media continues to be fertile soil for ideologies and groups that prosper in an environment where truth can be sold to the highest bidder.

### **Who exactly is carrying out SMDIO?**

Demographically, Mexico’s political trolls are often young people or students in need of extra income. According to two former trolls who spoke to El Pais on condition of anonymity, they earned about 12,000 pesos per month [665 USD] and were in charge of dozens of fake Twitter or Facebook accounts that used either fictitious or stolen identities.<sup>xxii</sup>

According to social media experts in Mexico, the armies of bots and trolls of the current election have evolved and “are no longer the only tools around.” Sergio Jose Gutierrez of Espora, a political digital communication company, states that parties now generate fake news and advertisements in websites allegedly devoted to news and are subsequently sold to the highest bidder. Experts such as Oxford University researcher Yin Yin Lu have also observed a rise in IO campaigns sending out malicious false news about candidates personal lives through WhatsApp and Snapchat, noting that “tactics like this are much more sinister and manipulative because they are an invasion of private life.”<sup>xxiii</sup>

The lucrative IO market in Mexico has also attracted actors such as Cambridge Analytica. In fact, according to the company’s own director general, it has already worked secretly in Mexico prior to this election.<sup>xxiv</sup> According to El Pais, political parties are provided \$360 million by the NEI, a large portion of which is used for “online campaigning.” With thousands of candidates competing for a seat in Congress, governorships, and the Presidency, digital consultancy firms such as

Cambridge Analytica have numerous opportunities to sign lucrative contracts. According to Alberto Escorcia, a fake news Twitter expert, SMDIO is “a big-money industry” and private competition must keep pace or else “16 and 17-year-olds will overtake [private] business.”<sup>xxv</sup>

The extent to which the political parties themselves are leveraging SMDIO is already apparent. Evidence exists that lower-skill hackers, not just high-profile ones such as Sepulveda, are growing in scale due to the lucrative nature of the work. The SMDIO landscape has devolved into a for hire industry with real individuals being paid thousands of dollars to influence the threat landscape.<sup>xxvi</sup> With profit as the driving factor, the probability of interference by private parties will increase significantly for the upcoming election.

### **What drives the effectiveness of SMDIO?**

The effectiveness of SMDIO is driven by Internet penetration. The Internet is the primary means through which young people in Mexico, an important segment of the electorate, engage in democracy. According to an August 2017 survey by the Internet MX Association, nearly six out of ten Mexicans feel that the internet brings them closer to democratic processes despite the influence of misinformation.<sup>xxvii</sup>

Moreover, SMDIO tools such as bots and trolls ultimately grow the prestige and recognition of public figures. As long as Facebook and Twitter do not significantly counteract them, they will continue to grow. According to Sergio Zaragoza, CEO of Boton Rojo, a Mexican digital consulting firm, bots and trolls are “one more weapon in the electoral battle, and any campaign that fails to use them will miss out.” Zaragoza concludes that: “Is it dangerous for democracy? Yes, but the digital war is won by appealing to emotions.”<sup>xxviii</sup>

### **Defensive Outlook and Response**

According to Lloyd Benton, a political risk analyst, the mentality in Mexico towards cyber defense is changing but not as quickly as hackers’ ability to develop means to carry out attacks. According to Defense IQ, cyber attacks in Mexico have increased exponentially over the last five years. Notable examples include government websites connected with Mexico’s 2012 presidential elections hit by hacktivists conducting DDoS attacks, XSS, SQL injections, and Anonymous Mexico disrupting the Mexican defense secretariat (SEDENA) website in 2013. Moreover, Critical National Infrastructure (CNI) has become increasingly dependent on ICS/SCADA which remain highly vulnerable to infiltration and disruption.<sup>xxix</sup>

However, in response to SMDIO and “fake news” dominating headlines prior to the election, the National Electoral Institute (NEI), Google, Facebook, Twitter, and civil society have partnered on a project called #Verificado2018, an alliance of 60 Mexican media outlets, universities, and non-profit groups launched to check facts and flag false information.<sup>xxx</sup> The exhibit below illustrates the scope and reach of the project.



## UNA ALIANZA NACIONAL

#Verificado2018 está conformado por periodistas de todo el país, organizaciones de la sociedad civil y universidades. Este mapa da cuenta de la representación que se tendrá a través de los medios de comunicación en los estados de la república.

*“A National Alliance” dedicated to fighting fake news composed of academics, civil society, and government entities.*<sup>xxxi</sup>

Moreover, in March 2018 Facebook purchased ads in prominent Mexican newspaper El Financiero detailing “Tips to Detect Fake News” with tips such as “Doubt the Headline” and “Check the Source.”<sup>xxxii</sup>

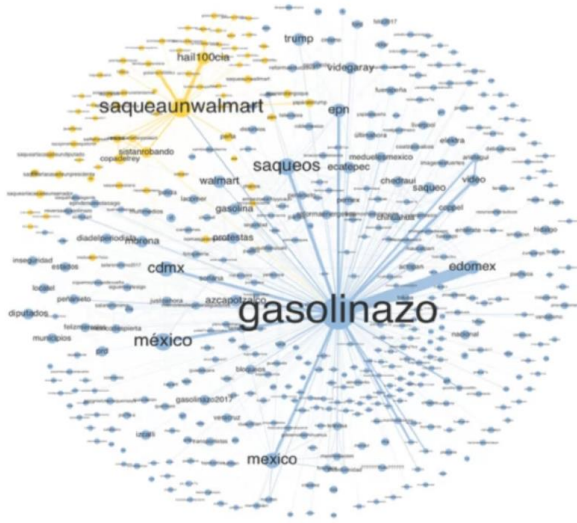
**Consejos para detectar noticias falsas**  
Nos tomamos muy en serio las noticias falsas. Descubre algunas formas de identificarlas.

- Duda de los títulos**  
Las noticias falsas suelen presentar títulos llamativos, escritos en letras mayúsculas y con signos de exclamación. Si un título contiene afirmaciones sorprendentes y poco creíbles, es probable que se trate de información falsa.
- Observa con atención la URL**  
Una URL falsa o que imita una original puede ser una señal de advertencia. Muchos sitios de noticias falsas realizan pequeños cambios en la URL de fuentes de noticias auténticas para evitarlas. Puedes visitar el sitio oficial y comparar la URL.
- Investiga la fuente**  
Asegúrate de que la noticia esté escrita por una fuente de confianza respaldada por una reputación de exactitud en la información. Si la noticia proviene de una organización desconocida, verifica la sección “información” para obtener más detalles.
- Detecta si el formato es poco común**  
Muchos sitios de noticias falsas tienen errores ortográficos o diseños extraños. Identifica estas señales.
- Presta atención a las fotos**  
Las noticias falsas suelen contener imágenes o videos manipulados. En ocasiones, es posible que la foto sea auténtica, pero que la hayan sacado de contexto. Puedes buscar la foto o imagen para verificar de dónde proviene.
- Comprueba las fechas**  
La cronología que usan las noticias falsas puede resultar ilógica o incluso pueden estar alteradas. Las fechas de los acontecimientos.
- Verifica las pruebas**  
Comprueba las fuentes del autor para confirmar que sean precisas. Si no se aportan pruebas o se confía en expertos cuya identidad no se menciona, es posible que la noticia sea falsa.
- Consulta otros informes periodísticos**  
Si ningún otro medio informa sobre la misma noticia, es posible que sea falsa. Si aparece en varias fuentes de confianza, es más probable que sea verdadera.
- ¿La noticia es un engaño o una broma?**  
En ocasiones, suele ser difícil distinguir una noticia falsa de una publicación humorística o satírica. Comprueba si la fuente de donde proviene suele realizar parodias y si los detalles y el tono de la noticia sugieren que puede tratarse de una broma.
- Algunas historias falsas tienen una intención**  
Reflexiona sobre las noticias que lees y comparte solo las que sabes que son creíbles.

Juntos, podemos limitar la difusión de noticias falsas.

*“Tips to Detect Fake News”*

## Primary Targets of SMDIO



*Signa Labs data cluster showing the troll offensive of "#saqueaunwalmart: connected to #gasolinazo*

While the strategic target of SMDIO is the electoral process, the primary individual targets are journalists/activists, political movements, and political parties. In 2010, Mexican journalist and internet activist Alberto Escorcia noticed several accounts posting derogatory messages at supporters of a union strike, all repeating the same message with profile photos of attractive people from other countries.<sup>xxxiii</sup> Escorcia began documenting a “veritable troll boom” the following year during Mexico’s presidential elections and realized that “it was the start of a new war in Mexico and the internet was the new paradigm.”<sup>xxxiv</sup>

As an expert on bots and trolls, Escorcia receives regular death threats and has been physically attacked in public. According to Tanya O’Carroll, a technology and human rights adviser for Amnesty International who recently published an investigation of political impact and influence of trolls and bots in Mexico:

The emerging pattern of well-funded and sophisticated cyberattacks and misinformation campaigns online are fueling this climate of fear and silencing those who speak out. It is time that Twitter recognizes their platform has become a weapon in Mexico and it is being used to silence and punish critical voices. Instead, they are choosing to ignore the presence of orchestrated troll networks on their platform and behave as if it were somebody else’s problem. The company can and must do more.<sup>xxxv</sup>

In addition, bot armies attempt to influence and control the political conversation during movements such as #YaMeCanse or “I am fed up” (the most used hashtag in Mexican history) and “gasolinazo.” In the case of the latter, automated accounts began tweeting the hashtag along with the hashtag “#saqueaunwalmart” to encourage people to “sack a WalMart” as a sign of protest. The data cluster above illustrates the #saqueaunwalmart bot activity connected to #gasolinazo:<sup>xxxvi</sup>

They also retweeted #YaMeCanse with links to pornography or violent photos with the intent that Twitter would flag the hashtag and block it. According to Escorcia, a repentant troll operator approached him in 2014 out of guilt and confessed to having been paid 50,000 pesos an hour (almost USD \$2,500) to run up to 150 accounts against Mexico’s #YaMeCanse protests. The orange growth in the exhibit below illustrates the troll offensive against #YaMeCanse:<sup>xxxvii</sup>



The orange smudge at the top is the start of the troll offensive against #YaMeCanse. The protesters had to change to #YaMeCanse2, and then 3, all the way to 33, in order to stay ahead of the trolls who flooded the hashtag with spam.

### **SMDIO and the Voting Process**

In Mexico, citizens vote at paper ballot (not electronic) voting stations assigned based on one's address. In order to vote, citizens must register before the election and obtain a voter ID card that includes their photograph, name, address, fingerprint and age. While this is an effective means to ensure that a voter does not impersonate another singular person, it does not prevent other means of influence such as absentee ballot fraud, coercion, vote buying, fake registration forms, or voting from the wrong address.

Therefore, political parties and outside actors can still conduct SMDIO to influence voters through misinformation and intimidation. In addition, the 2018 election will be the first in which voters can register for absentee ballots online. Given that this is the initial rollout of the online system, there exists a possibility of voter fraud by "Mexican voters" located abroad i.e. Russia. To counteract this, the National Electoral Institute (INE) has stated that it will reinforce its cybersecurity systems in cooperation with UNAM (National Autonomous University of Mexico) and external auditors.<sup>xxxviii</sup>

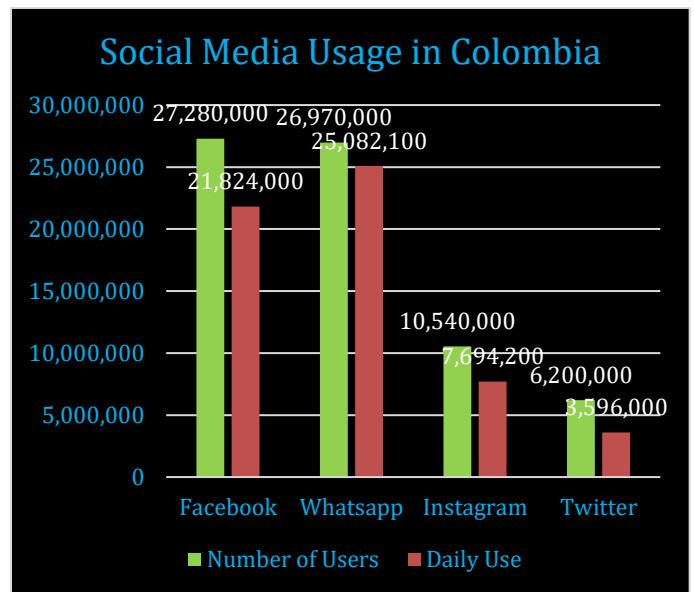
## Case Study: IO in Colombian Elections

### Context

Similar to Brazil and Mexico, the threat of SMDIO existed well prior to the upcoming Colombian presidential elections. With a diverse voting electorate and a population increasingly connected to the Internet, Colombia is fertile ground for SMDIO. Allegations of SMDIO were common following the 2016 peace accord plebiscite with the Revolutionary Armed Forces of Colombia (FARC) and new allegations surround the May 2018 presidential elections. While awareness surrounding the threat has increased, cybersecurity development and legislation remains far behind, increasing the likelihood that Colombia's upcoming Presidential elections will be affected by SMDIO.



We Are Digital, 2018



Colombian Ministry of Technology and Communications, 2016.

### Social Media Usage Statistics

As the second largest country in South America, Colombia has become an important digital market as more of the population is connected to the Internet. With a digital penetration rate of 63% (31 million users), Colombia is the fourth most connected country in Latin America.<sup>xxxix</sup> This includes 29 million social media users, of which the majority are active users.<sup>xi</sup> Just as in other countries, social media usage is dominated by Facebook, and messaging is dominated by WhatsApp, which plays an increasingly important role in the dissemination of SMDIO. In the case of WhatsApp, the Colombian Ministry of Technology and Communications cited daily usage rates as high as 93%.<sup>xi</sup> YouTube also plays an increasingly important role in the dissemination of



We Are Digital, 2018



SMDIO as it was one of the most visited Colombian websites in 2017, dominating all other web traffic in time per visit.<sup>xlii</sup>

## Recent History of IO in Colombia

### 2016 Plebiscite on the FARC Peace Process

While Colombian hacker Andres Sepulveda is most well-known for his Mexican election IO campaigns, he was jailed for his activities related to the 2014 Colombian Presidential election, hacking emails belonging to government officials during peace negotiations with the FARC.<sup>xliii</sup> Sepulveda was working for the conservative Centro Democratico party, who was fiercely opposed to the peace negotiations with the FARC and was attempting to garner insider information in an attempt to sway public opinion. Several Colombian Army generals were dismissed during the “Andromeda” scandal, which demonstrated the capability of rival government factions to attack each other utilizing cyber tools. This was apparent during the 2016 plebiscite, in which Colombian citizens voted whether to accept the government’s peace deal with the FARC. The passing of the plebiscite was perceived as a given, but the conservative party leveraged SMDIO to discredit and influence the peace process. This contributed to the eventual failure of the plebiscite.<sup>xliv</sup>

### Strategy

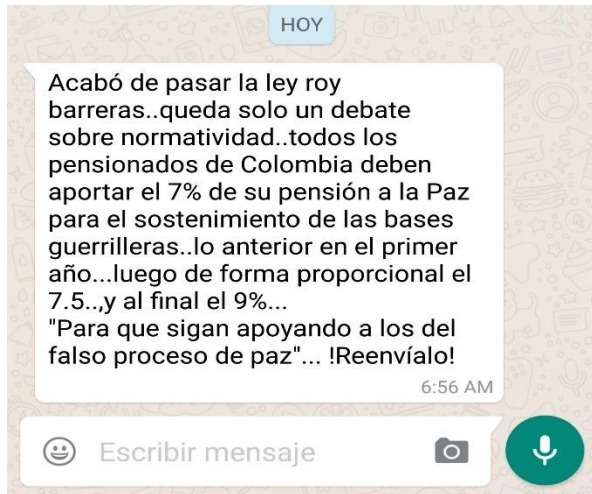
One of the chief strategists behind the campaign, the Centro Democratico’s Juan Carlos Velez, offered insight into the “NO” campaign’s methodology following the surprise victory of the “NO” vote. Velez stated that the campaign centered its messaging on indignation and shifted focus away from the actual content of the peace accords. The aim was to influence voters by making them angry rather than informed.<sup>xlv</sup> Once the campaign devised a general theme, they simply implied certain messages and let the viral nature of social media do the rest.



*“Do you want to see Timochenko as President? Vote yes for the plebiscite.”*

*Blu Radio Nacional, 2018.*

During a campaign trip within Colombia, Velez published an image of Colombian President, Juan Manuel Santos, alongside FARC leader, “Timochenko,” with accompanying text asking why money was going to be given to the FARC while the country was under economic duress. Within a short period, the Facebook post had 130,000 shares and reached 6 million people.<sup>xlvi</sup> Asked why his party focused on a campaign of distortion, Velez replied “Because it was the same thing done by the ‘YES’ campaign.”<sup>xlvii</sup> Followers of both sides became virtual armies of SMDIO who forwarded fake news and photoshopped images. Though campaign strategists devised a general theme, the campaign was executed predominantly by individuals who supported their position.



“The Roy Barreras law was just passed..only one debate concerning regulations is left..all the reitrees of Colombia will have to give up 7% of their pension to the peace process to sustain the guerilla bases..7% in the first year, increasing to 7.5%, and finally 9%..”So you keep supporting the fake peace process”

Forward this message!.”

Pulso.com,

2016.

erased. The implication was that people who voted against the plebiscite could have their votes changed after they voted.<sup>1</sup> The message went viral and Caracol had to run a television segment discrediting the false claims. However, responding to fake news and altering public perception after the exposure is far more difficult as the second mover. This message was popular enough to be recycled for the upcoming presidential elections. There is even a video on YouTube (with links sent via WhatsApp chains) claiming proof of the erasable pens. The National Registrar, Juan Carlos Galindo, uploaded a Twitter video debunking the claims and even told Colombian citizens to bring their own pens to vote if they had any doubts.<sup>li</sup>

While the billboard above was used as a popular marketing tool to promote fear, it was not an instance of fake news as it only implied possibility. Clearer examples of SMDIO were common throughout the plebiscite, the majority of which were disseminated through WhatsApp chain messages, such as the example to the left.

### Examples

The message began circulating following news reports that the Colombian Congress was considering raising taxes on pensioners that earned over a certain amount of income.<sup>xlviii</sup> It falsely claimed a new law was passed by a Colombian Senator reducing pensions to fund the reintegration of demobilized guerillas.<sup>xlix</sup> The measure, which was not passed, had nothing to do with the peace process, but was seized as an opportunity by the “NO” campaign to distort factual news in order to promote their agenda. SMDIO utilizing this tactic is more likely to be believed because the target audience has already been exposed to the original, factual news article.

Another false news report that circulated through SM and WhatsApp was a message claiming that Colombian News outlet, Caracol, demonstrated that pens used during the plebiscite vote could be easily



Miguel Pajón L.  
@pajonmiguel

REITERO: @marianapajon NO PERTENECE A NINGUNA CAMPAÑA NI PARTIDO POLÍTICO POR FAVOR NO ALTEREN NI UTILICEN SU IMAGEN

13:25 - 12 sept. 2016

1.393 1.665 personas están hablando de esto

Another popular method during the plebiscite was photoshopping existing images in order to create the illusion of sponsorship by celebrities. The example to the left shows the original, as well as the manipulated image of Colombian Olympian Marian Pajon, which was later denounced by her brother/manager. While each of these examples is demonstrative of the “NO” campaign’s efforts, they were not the only party to utilize SMDIO. For example, a photo of former Colombian President and head of the Centro Democrático Party, Alvaro Uribe, was photoshopped to display him with a placard supporting the plebiscite.

The question remains: did the “NO” campaign’s SMDIO influence the vote? Many individuals likely voted along party lines, but with a razor-thin victory margin for “NO” of 55,651 votes (or .4%), it is likely that SMDIO was a deciding factor.<sup>lii</sup>

*“I’m Winning Thanks to you.”*

*“No to the Peace Plebiscite!”*

*Pulzo.com*

## Current IO Landscape in Colombia

### Competing Claims

The current SMDIO landscape of Colombia is very similar to 2016. WhatsApp chain messages are still extremely popular, while Facebook and Twitter are used to spread disinformation concerning the upcoming elections. During the first Presidential debate, leftist candidate Gustavo Petro stated there were two campaigns being run: one visible and the other a shadow campaign. “The second [shadow campaign] is the Cambridge Analytica Way. Those methods are paid for with a lot of money, and in Colombia today, there have been significant investments to construct a campaign that is defamatory, dirty, and low, in order for one of the candidates to win.<sup>2</sup>” Petro also referenced the plebiscite when describing what was going on in the current elections:

“Candidates don’t appear in the shadow campaigns, that is where the anonymous appear on social networks. There are thousands, tens of thousands of robots, of people, of money that is used to manipulate public opinion. And they manipulate through tricks and falsehoods, preying on peoples’ instincts and passions. How did ‘NO’ beat ‘YES’? That’s how! A dirty campaign telling people the FARC was going to take over the country, telling people they were going to take all the taxi jobs away from taxi drivers, etcetera.”<sup>3liii</sup>

<sup>2</sup> *...el Segundo es el del Cambridge Analytica. Esos se pagan con mucho dinero, y en Colombia hoy, se ha invertido muchísimo dinero en la construcción de una campaña difamatoria, sucia, rastrera, y baja...tratando que gane uno de los candidatos.*

<sup>3</sup> *Que no aparecen las Figuras prestantes, ahí aparecen en las redes los anónimos, son miles, decenas de miles de robots, de personas, de dineros que van manipulando la opinión Y la van manipulando a partir del engaño y la falsedad, los bajos instintos, las pasiones. Como gano el no sobre el si? Así! Una campaña baja, rastrera diciendo que las FARC se iban a tomar el país, diciendo que le iban a quitar los taxis a los taxistas, etc.*



### Iván Duque

Tendencia de crecimiento en Twitter entre el 11 de diciembre y el 5 de enero:  
Estable

84%

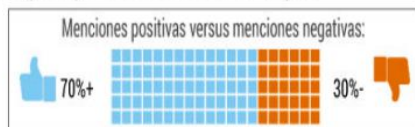
Porcentaje de seguidores reales en Twitter:



Fluctuación de fans en Facebook:

Incremento de 600 semanales para llegar a **34.939**

Países de origen sospechoso de fans de Facebook: Ninguno



### Gustavo Petro

Tendencia de crecimiento en Twitter entre el 11 de diciembre y el 5 de enero:  
Estable

60%

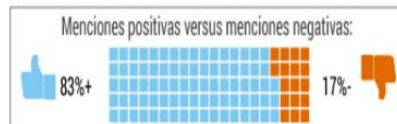
Porcentaje de seguidores reales en Twitter:



Fluctuación de fans en Facebook:

Incremento de 2.251 semanales para llegar a **888.346**

Países de origen sospechoso de fans de Facebook: Turquía, Irak, Paquistán.



#### Ivan Duque

Growth of Twitter Users between 11 Dec and 5 Jan: Stable  
Percentage of Real Followers on Twitter: 84%  
Fluctuation of Fans on Facebook: 600 gained per week for a total of 34,939

Suspicious Countries of origin of Facebook followers: None.  
Positive Mentions versus Negative Mentions

*El Espectador, 2018*

#### Gustavo Petro

Growth of Twitter Users between 11 Dec and 5 Jan: Stable  
Percentage of Real Followers on Twitter: 60%  
Fluctuation of Fans on Facebook: 2,251 gained per week for a total of 888,346

Suspicious Countries of origin of Facebook followers: Turkey, Iraq, Pakistan.

Positive Mentions versus Negative Mentions

*El Espectador, 2018*

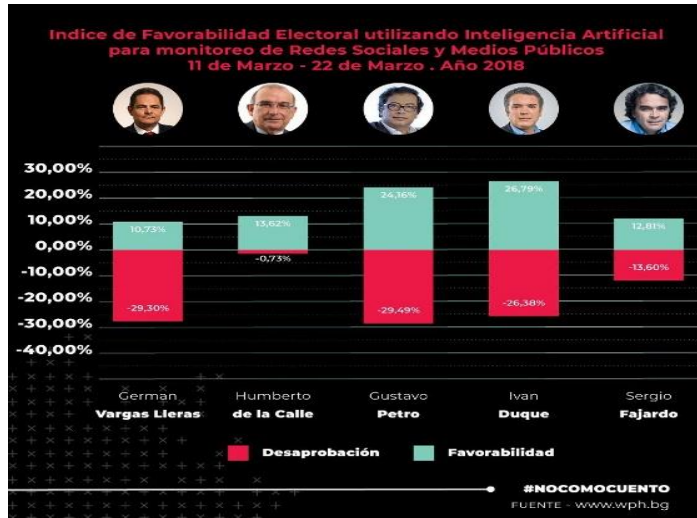
A spokesperson for the Centro Democrático (the party of Iván Duque, Petro’s rival) replied with, “If we look at the social networks, there is a lot of dirty campaigning going on, specifically the campaign of Gustavo Petro. They constantly create messages to confuse the populace... They have teams specifically focused on black campaigning, AKA disinformation.”<sup>4liv</sup>

Both main candidates in the upcoming presidential election accused the other of utilizing SMDIO. The analysis of Colombian cyber security firm Adalid and Noor showed tens of thousands of Twitter bots following the main presidential candidates’ Twitter feeds.<sup>lv</sup>

The study, conducted from 11 December 2017 to 5 January 2018, analyzed the authenticity of the candidates’ followers on Facebook and Twitter and measured whether content related to the candidates was positive or negative. For the content analysis, the study only measured the most popular 30% of the accounts following the candidates to measure influence.<sup>lvi</sup> It is uncertain what effect such large followings of bots will have on the elections, but if the 2016 U.S. Presidential elections are any indication, they may be utilized to spread or increase attention to SMDIO. Moreover, these bots are easily procured, as an official from the cyber unit of the Colombian

<sup>4</sup> Si revisamos en redes sociales, es mucha la campana negra que usan, específicamente de la campana de Gustavo Petro. Hacen Constantemente montajes bastante Fuertes para confundir a la gente.

National Police stated that, “Investigations from the Attorney General’s office have detected web sites that offer ‘packets of followers’ on social media platforms in order to generate trending topics, which allows a social media account to generate followers in a short amount of time. These packets, depending upon the price paid, guarantee from 1,000 to 100,000 followers. These services on the web are also offered to spread fake news.”<sup>lvii</sup>



*Electoral Favorability Index utilizing Artificial Intelligence to Monitor Social Networks and Media Outlets 11 March – 22 March 2018.*

*Red: Disapprove    Teal: Favorable*

*Inteligencia Artificial Electoral, 2018*

More recent statistics in the exhibit to the left from Inteligencia Artificial Electoral 2018 show the latest trends of candidates’ social media mentions. The data displays Petro and Duque as the candidates benefitting the most from social media positive mentions, as well as two of the top three that have the most negative mentions.<sup>lviii</sup>

While it is difficult to attribute SMDIO to candidates, J.J. Rendon, the aforementioned political consultant known as the “king of black propaganda” has clearly stated his intentions regarding Colombia’s upcoming elections. Rendon has stated that he is doing everything in his power to ensure Leftist candidate Gustavo Petro does not win. He claims that he is working of his own accord, utilizing his own digital and financial resources, and is independent of any political campaigns to promote Duque’s reputation and damage Petro’s.<sup>lix</sup> Rendon also claimed a personal

vendetta against the “Left” and claimed responsibility for an extreme leftist candidate’s, Piedad Cordoba, withdrawal from the Colombian Presidential election. In addition, he claims to be undermining the current front runner leftist candidate, AMLO, in Mexico.<sup>lx</sup>

### **Tactics: Disinformation**

Congressional elections in March 2018 have provided a preview of the SMDIO tactics to expect in the May presidential elections. According to Camila Zuluaga, a Colombian journalist and one of the founders of an organization dedicated to fighting fake news, the current election is at risk from similar SMDIO utilized in the plebiscite. “These IO campaigns utilize a variety of digital media sites... in order to give the message visibility. Putting the message out on several sites gives the message credibility, and from there it spreads to social media, where it becomes viral.”<sup>lxi</sup> Zuluaga does not believe the most impactful messages are the work of amateurs, due to the tailored nature of the messages and the prevalence of marketing firms offering such services. These firms often use intermediaries in order to mask the true identity of the client. According to analysis from Zuluaga’s organization, No Como Cuento, WhatsApp is currently the most popular platform utilized to conduct SMDIO.<sup>lxii</sup>



*Venezuelan Brother! Colombians aren't to blame for what is happening in your country, it's the Maduro government who you should demand. In Colombia we already have too much violence, please don't bring more, that doesn't work for us. They say that Venezuelans with Colombian IDs will vote for the Left. They think that if the FARC win, they will apply the same politics that Chaves and Maduro applied and which have made Venezuela into what it is today, which is the reason you had to flee. If you support the FARC, you won't have anywhere to go to ask for help, because both countries will be the same.*

*Pulzo.com, 2018*

## Examples

One of the most popular SMDIO messages targeting the upcoming elections provides a prime example of a message's ability to cross SM platforms once it becomes viral. The WhatsApp message warned that Venezuelan refugees living in Colombia would be allowed to vote during the Congressional and Presidential elections. This incited fear that the refugees would vote for leftist candidates and turn Colombia into the next Venezuela.<sup>lxiii</sup> The message became viral enough that messages began appearing on Facebook pleading for Venezuelans not to vote for the Left, resulting in the Ministries of Interior and Migration publicly debunking the falsehood.<sup>lxiv</sup>

## Threat: Cyber Attacks

While the public discourse has been focused on social media threats, the cyber realm contains other potential threats to the upcoming Colombian elections. In early March 2018, the Colombian Minister of Defense, Luis Carlos Villegas, announced that the National Civil Registration page (organization in charge of elections in Colombia), suffered cyber-attacks just three days before Congressional elections.<sup>lxv</sup> Four attacks attempted to knock the National Civil Registration's page offline, of which three originated from within Colombia and one from Venezuela. In addition, within a week of the elections there were 59,000 attacks on pages associated with the National Civil Registration and other electoral services.<sup>lxvi</sup> This is not the first time the Civil Registration page has come under attack. Colombian President, Juan Manuel Santos, signaled in January of 2018 that the National Civil Registration was the target of numerous cyber-attacks during the 2016 plebiscite.<sup>lxvii</sup>



*You know what? @IvanDuque don't celebrate in my land the triumphs of the paramilitaries. Their only flavor is of cocaine and genocide.*

*Pulzo.com, 2018*



*Doctor @petrogustavo instead of spreading fake videos to promote hate between Colombians, I'm sharing the real video of the Cold Drop. We sing to the hope and future of Colombia.*

*Pulzo.com, 2018*

Candidates often find themselves entangled in disinformation campaigns. In early April 2018, leftist candidate Gustavo Petro shared a video on his Twitter page of Conservative Candidate Ivan Duque singing a traditional Colombian song. At the end of the song, someone apparently yells, “Long live the paramilitaries!”. Support of paramilitary groups is problematic in Colombia due to their history of drug trafficking and murders. Petro criticized Duque for promoting paramilitary groups. However, the video was edited. Duque shared the unedited video minutes later which did not include praise of the paramilitary groups. Petro issued an apology for the dissemination of the fake news, but not before the edited video had been shared extensively by his followers.<sup>lxviii</sup> Such instances have been common in the SMDIO landscape. As a result, candidates have discovered two things: (1) SMDIO can be a double-edged sword (Petro was heavily criticized by the media for the dissemination of fake news), and (2) they rarely have control over the spread of an idea via SMDIO once it is planted in the minds of the public.

### **Threat: External Interference**

In January 2018, Frank Mora, the former Deputy Assistant Secretary of Defense for the Western Hemisphere, claimed that Russia is trying to interfere in the Presidential and Congressional elections in Colombia.<sup>lxix</sup> Mora, along with the National Endowment for Democracy, has been monitoring the Colombian elections and believes that Russia is utilizing SMDIO to generate confusion and distrust in the electorate. Mora has not identified a Russian preference for any candidate but believes the IO campaign is utilizing similar tactics seen in the U.S. Presidential elections. He believes that Russian interference is aimed at creating conflict between the U.S. and Colombia and weakening the relationship between the two countries.<sup>lxx</sup>

According to a 2018 Senate Foreign Relations Committee report detailing Russia’s Influence Operations targeting elections in Europe, Russia would likely utilize similar tactics if they targeted elections in the Western Hemisphere. These tactics could include “overt and covert support for far

left and right political parties... and focus on exploiting internal discord in an effort to break centrist consensus on the importance of core institutions.’<sup>lxxi</sup>

The evidence of this is borne out by the numbers as RT en Espanol has expanded its presence in LA and now has approximately 350 employees, 5.8 million Facebook followers, and 2.8 million Twitter followers. A content analysis of RT en Espanol shows a network established to promote Russian interests and attack the West at every possible opportunity. Furthermore, the news outlet lends significant air time to antiestablishment groups, while omitting coverage critical of its Latin American allies such as Venezuela.<sup>lxxii</sup>

Given recent Russian resurgence and their goal of restoring their status as a great power, it is plausible that Russia would act to influence LA elections. This accomplishes two ends: first, it expands Russian influence in LA and second, it diminishes U.S. influence in the region. Although allegations of Russian influence have already been made, aside from a significant Russian investment in RT en Espanol, evidence of SMDIO targeting upcoming elections is currently circumstantial.



---

*Claudia: ELN Check Point, route to Molino, Villanueva, La Guajira. These terrorists know they are in control of the slow down, as crime increases, more awards for Santos!*  
*Colombian Police: This is FALSE, FAKENEWS, none of these acts have occurred in La Guajira, these images are from 2016. Break the Chain and always verify your primary sources of information.*  
*El Espectador, 2018*

---

### Overall Impact

The difficult question, not only in Colombia, is what tangible effect does SMDIO have on electoral results? According to Miguel Jaramillo, a consultant for Political and Government Marketing, big data is making it easier to find a tangible link between the two by enabling marketers to contact individuals directly through various SM platforms and find out who they actually voted for. This data is then compared to their social media habits.<sup>lxxiii</sup> With the recent Cambridge Analytica revelations, it is not surprising that marketing firms’ ultimate goal is to deliver hard metrics demonstrating links between their services and actual votes. According to Jaramillo, limited research demonstrates that in Latin America, “Every 30 ‘Likes’ tentatively translates to one real vote.”<sup>lxxiv</sup> When one considers the slim margins that have decided recent elections (~50,000 votes), perhaps every “Like” matters.

### Government Response: Police

The Colombian National Police has begun a counteroffensive against false claims made by candidates on social media in an effort to combat SMDIO. In February of 2018, Centro Democratico Senator Claudia Bustamante posted a photo of a 2016 farmer’s strike and falsely claimed that the National Liberation Army (ELN) was burning trucks as part of a national slow down.<sup>lxxv</sup> The CNP immediately denounced the message as fake news in order to slow down the spread of the message.



### Government Response: Elections

Colombian President Juan Manuel Santos, announced in January of 2018, the creation of an electoral intelligence unit in an effort to defend against cyber-attacks targeting the Colombian elections. Santos also used the announcement to raise awareness of the threat.

To guarantee that these upcoming elections are the most secure, the Integrated Center for Electoral Intelligence (CI3E) has been created, in which the vulnerability and risks for the upcoming elections will be evaluated in all of the country's 1102 municipalities... With the importance of technology, new threats against democracy have sprung forth through cyber-attacks... Information is circulating suggesting possible attacks, which may even come from abroad. Last Friday, along with the National Registry, the National Police, the military, and the Ministry of Telecommunications, we activated a Joint Command Post to strengthen preventive measures and confront any digital security threat during the 2018 elections. It includes consultants that are experts in digital and information security. We are going to activate a call center for cyber incidents the upcoming week which will include a toll free 1-800 line. **The attacks against democracy are not only focused on our electoral system. They are also related to the diffusion of false information, of lies that aim to garner fear or generate distrust, and to manipulate voters. Because of this, guaranteeing a political debate and serious elections that are transparent, but without manipulations and falsehoods, is an assignment for all of us: the government, campaigns, political parties, the media, and citizens.** In this purpose it is fundamental the role that the media and journalists play. I invite you to evaluate and denounce, as you have been doing, any intent to manipulate and disorient public opinion.<sup>5lxxvi</sup>

The Colombian Minister of Defense also signaled that the CNP and Justice Department have formed a special group aimed at stopping electoral sabotage emanating from the Internet. This includes SMDIO threats and profiles that publish threatening messages will be identified, closed, and the account owners will be held accountable.<sup>lxxvii</sup>

---

<sup>5</sup> A su vez, para garantizar que estas sean las elecciones más seguras, se creó el Centro Integrado de Inteligencia Electoral CI3E, en el cual se hace la evaluación de vulnerabilidad y riesgo para las elecciones en los 1102 municipios del país. En el mundo de hoy, con la importancia de la tecnología, surgen nuevas amenazas contra las democracias a través de los llamados ciber ataques. Está circulando información de posibles ataques o intenciones no sanctas que podrían provenir incluso del exterior. El viernes pasado, junto con el Registrador Nacional, la Policía Nacional, las fuerzas militares y el Ministro de las TIC activamos un Puesto de Mando Unificado para robustecer las medidas preventivas y enfrentar cualquier amenaza de seguridad digital durante las elecciones de 2018. Contará con la asesoría de asesores expertos en seguridad informática y digital. Vamos a activar un centro de atención de incidentes cibernéticos la semana entrante que contará con una línea de atención telefónica gratuita 1-800. Los ataques contra la democracia no están dirigidos únicamente contra el sistema electoral. También tienen que ver con la difusión de información falsa, de mentiras que buscan atemorizar o generar desconfianza, y así manipular a los electores. Por esto, garantizar un debate político y electoral serio, transparente y democrático pero sin manipulaciones y falsas verdades es una tarea en la que debemos comprometernos todos: el gobierno, las campañas, los partidos, los medios, la ciudadanía. En este propósito es fundamental el papel que cumplen los medios de comunicación y los periodistas. Los invito a que evalúen y denuncien –como lo han venido haciendo—cualquier intento para manipular y desorientar a la opinión.

### **Law**

Currently, disseminating fake news or utilizing SMDIO is not illegal. However, Law 224 was proposed in 2017, which would have made the creation of false or anonymous social media accounts illegal if they were used to cause injury or calamity, violate a person's privacy, or to disseminate fake news with the intent to cause calamity or confusion in the general population.<sup>lxxviii</sup> The law was never voted on but did raise concerns about the fine line between political censorship and what defines an appropriate response to SMDIO threats.

### **Civil Society**

Organizations such as the one started by Colombian journalist Camila Zuluaga, "No Como Cuento," have partnered with the Colombian government to spread awareness regarding fake news. While not financially supported in order to maintain transparency, various Colombian government websites have retweeted/shared the organization's messages to expand their reach on social media. There are now multiple organizations dedicated to combatting SMDIO which has now garnered widespread coverage ahead of the May elections. Newspapers and television shows have dedicated segments aiming to inform the public. SM campaigns have been deployed to debunk fake news and encourage citizens to educate themselves in order to counteract SMDIO.

### **Outlook**

Taking into account past and current SMDIO campaigns related to elections, the rise of companies or individuals offering such services online, and the limited means of the Colombian government, **it is highly likely that SMDIO campaigns are currently targeting the upcoming presidential elections and will remain part of the threat landscape for the foreseeable future.**

## **Case Study: IO in Brazilian Elections**

### **Context**

Brazil is the largest geographic country in South America and commands the eighth largest economy in the world<sup>lxxxix</sup>. Its government is steward to the lives of more than 207,353,000 people.<sup>lxxx</sup> By 2016, there were about 140 million internet users in Brazil, making it the largest internet market in Latin America and the fourth largest internet market worldwide.<sup>lxxxix</sup> On October 7, 2018 Brazil's general election for the Presidency, two thirds of its federal Senate seats, state governorships and local assembly will take place. All 513 Chamber of Deputies<sup>6</sup> seats will be contested.

The Brazilian elections are being held at a time of great vulnerability for democratic electoral politics. The ongoing corruption prosecutions, known collectively as the “Carwash Operation” have polarized society. In April, the leading 2018 contender and former President, Lula, was imprisoned. Whether or not he can run remains an open question. These dramatic events and unresolved questions create fertile ground for SMDIO.

The collection of actors aiming to counteract SMDIO ahead of the 2018 Brazilian elections has engendered overlapping and, at times, conflicting interests. The Supreme Court, the Public Ministry, the National Congress, the military, civil society and others assume varying degrees of responsibilities in securing the integrity of the electoral process. The crowding of legislative, law enforcement, judicial, political, and intelligence agency priorities encourages an ad-hoc, confused, and ultimately inadequate response to the threat of SMDIO.

Brazil has been at the vanguard of informational freedom and civil liberties tangential to internet policy for decades. Their civil society's “focus on Internet public policy issues is highly sophisticated, the product of debate within Brazilian society over how to address issues such as cybercrime, privacy, net neutrality, digital access, and spam that began in the late 1990s.”<sup>lxxxix</sup> Their famously progressive national internet legislation – The Marco Civil da Internet – represents a model of internet governance relevant to not just the largest country in Latin America, but the future of global internet legislation. It has proven to be the main vehicle for judicial remedies against SMDIO.

### **Social Media Usage in Contemporary Brazil**

Since the spread of mobile technology at the turn of the millennium, internet access in rural and semi-urban areas has exploded. By January 2018, there are over 139 million internet users in Brazil, including 130 million active social media users. The number of mobile users in Brazil by January 2018 reached 143 million and almost 68% of Brazilians are connected online through mobile access.<sup>lxxxiii</sup>

The dominant platforms in Brazil include Facebook, WhatsApp, Google+, Instagram, Skype, Twitter and LinkedIn, according to the report *Computational Propaganda in Brazil: Social Bots During Elections* published by the University of Oxford.<sup>lxxxiv</sup> ComScore, a global marketing and data analysis firm, estimates that Brazilian users spend over 95% of their social media time on Facebook.<sup>lxxxv</sup>

WhatsApp is the most popular means of communication in Brazil. Most other SM usage stems from Brazilians “using WhatsApp groups to drive people to more public forums on places like

---

<sup>6</sup> *Câmara dos Deputados*

Facebook and Twitter.”<sup>lxxxvi</sup> Because of its opacity, WhatsApp is the least accessible in terms of research and reporting. This opacity makes Brazil more vulnerable to the spread of fake news and is one of the main SMDIO challenges facing the country.

### **Recent History of SMDIO in Brazil**

In the research paper published by University of Oxford’s *Computational Propaganda Project*, the 2014 presidential election witnessed some of the earliest cases of botnet-supported SMDIO. The fake news spread by bots spiked sharply during the 2014 debates between former Brazilian President Dilma Rousseff and opposition leader Aécio Neves.<sup>lxxxvii</sup> According to O Globo, one of the largest media outlets in Brazil, 25% of the news during the 2014 election campaign was identified as fake.<sup>lxxxviii</sup> In that election, the most shared fake news stories attacked the candidates’ personal histories, political stands, and private lives. Rumors that “Rousseff used to be a bank robber” or that “Neves is addicted to cocaine” were widely disseminated using SMDIO.

“[Social Media] has an ever-growing influence in Brazil. Since 2010, we have been able to observe the development of robots that artificially inflate the candidates' agenda, especially [on] Twitter,” said Tai Nalon, founder and president of Aos Fatos, the largest political fact-checking platform in Brazil. “It’s not possible to say that this kind of activity has a decisive weight on people's votes, but it certainly have the potential to influence debates and guide gatekeepers,” she added.<sup>lxxxix</sup> Even though Brazilian election laws strictly prohibit campaigns from deploying third party automated marketing tools such as SM botnets and paid influencers, these practices were pervasive.<sup>xc</sup>

The electoral law was modified in 2015 after the deluge of fake news exposed during the previous year’s presidential election, emphasizing that accounts promoting campaign messages on social media must be operated by an individual human. However, the legal response is still viewed as inadequate. “The fact is that Brazil's institutions are unprepared to handle abuse in the digital field. The law is always behind technological advances,” said Nalon.<sup>xc</sup>

One year after the 2014 Election, Brazil witnessed another spike of fake news because of Operation Lava Jato, one of the largest anti-corruption investigations in the world, and the simultaneous impeachment of President Rousseff. The former President was found guilty of moving funds between public budgets to fix the deficit caused by popular social programs.

O Globo, Brazil’s largest television channel, has long claimed that both Rousseff and Lula were involved in the massive corruption scandal. In 2017, the network admitted that they had inadvertently spread fake news about Rousseff during the impeachment. O Globo journalist William Waack said the previous reports about Rousseff owning offshore accounts were inaccurate.<sup>xcii</sup>

## Current SMDIO in Brazil

There is a multitude of contemporary examples of fake news stories pervading Brazilian SM today. One recent example played out between two global brands. “Pepsi outdid Coca-Cola in sales because an image of Jair Bolsonaro [was] stamped on the cans of soda from the brand. The ‘news’, published on December 4<sup>th</sup> on the site Current News, was reproduced in five Facebook pages with a total of 1.8 million followers. In a few days, it had more than 20,000 ‘likes’ and a considerable number of shares.”<sup>7 xciii</sup>

News outlet VEJA performed one of the most recent polling efforts to determine the velocity of fake news in the general population. “Exclusive research done at the request of VEJA by the consultancy Ideia Big Data, with 2,004 people interviewed by phone between January 9<sup>th</sup> and 10<sup>th</sup> [2018], showed that 83% of those interviewed had shared fake news in their social networks and WhatsApp groups.<sup>8 xciv</sup> In another poll which examined 534 verifiably false articles from dozens of sites known for spreading fake news, it was “found that the preferred targets of the lies are, in order, ex-President Lula, President Michel Temer, and the judge [heading the Lava Jato prosecution] Sergio Moro.”<sup>9 xcv</sup>



A photo of the well-known figure surfaced that claimed, “the judge was bent over the Bible after having announced the condemnation of Lula...” implying his emotional torpor upon sentencing Lula. Though the photo was real, the true context of the image was the judge trying to find an electrical outlet under the table to recharge his laptop.”<sup>10 xcvi</sup>

“Snap of Sergio Moro After Judging Lula Touches Brazil – He Stayed Like This for 40 Minutes.” *Veja.abril.com.br* (13 Jul 2017)

<sup>7</sup> “A Pepsi superou a Coca-Cola em vendas porque a imagem de Jair Bolsonaro passará a estampar as latinhas de refrigerante da marca. A “notícia”, publicada em 4 de dezembro no site News Atual, foi replicada em cinco páginas do Facebook com um total de 1,8 milhão de seguidores. Em poucos dias, ela teve mais de 20 000 curtidas e um número considerável de compartilhamentos.”

<sup>8</sup> “Pesquisa exclusiva feita a pedido de VEJA pela consultoria Ideia Big Data, com 2 004 pessoas ouvidas por telefone entre 9 e 10 de janeiro, mostra que 83% dos entrevistados temem compartilhar notícias falsas em suas redes sociais e grupos de WhatsApp.”

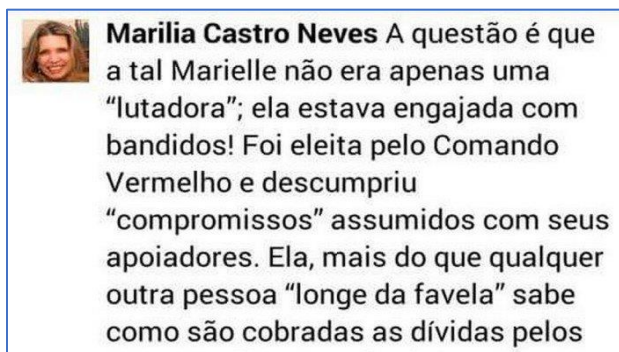
<sup>9</sup> “constatou que os alvos prediletos das mentiras são, pela ordem, o ex-presidente Lula, o presidente Michel Temer e o juiz Sergio Moro.”

<sup>10</sup> “Uma em que o juiz Sergio Moro aparecia numa foto sentado em uma cadeira e curvado sobre a mesa. O texto dizia que o juiz estava debruçado sobre a Bíblia depois de ter anunciado a condenação de Lula — a foto era real, mas a intenção do magistrado com o gesto era bem outra: ele procurava uma tomada sob a mesa para recarregar seu laptop.”

## The Case of Marielle Franco

The progressive Rio de Janeiro councilwoman Marielle Franco was assassinated on March 14<sup>th</sup> of 2018. She was an outspoken and controversial figure with very progressive politics. Her death ignited a political firestorm, both in cyberspace and reality. In an indication of the volume of posting online, the Director of Analysis of Public Policy of the Getúlio Vargas Foundation said that, “according to the institution, Marielle was the theme of 2.14 million tweets between the night of the 14<sup>th</sup>, when she and her driver Anderson Gomes were assassinated, and midnight of Sunday, March 18<sup>th</sup>.”<sup>11 xcvii</sup> Twitter registered more than half a million mentions in the first 19 hours after her death.<sup>xcviii</sup>

Immediately following the killing, a litany of allegations was found in fake news headlines: “Pregnant at 16 years old. Married with Marcinho VP. Marijuana user. Elected by the Comando Vermelho [gang] and killed when she defied a rival gang.”<sup>12 xcix</sup> The fake news headlines were spread even by elected officials, intentionally or not: “A Rio de Janeiro judge, Marília Castro Neves, spread the fake news rumor by Facebook, that the councilwoman was elected by Comando Vermelho, one of Brazil’s most endemic and prolific gangs.<sup>c</sup> Supposedly this was done inadvertently. Later, the judge walked back her post, claiming that she “read it in a text from a friend”.<sup>13ci</sup>



*Marília Castro Neves, Rio de Janeiro Court Justice, Facebook Post: “The question is not whether Marielle was a ‘fighter’; she was in cahoots with bandits! She was elected by Comando Vermelho and failed to comply with prior ‘agreements’ with her supporters. She, as much as any other person ‘far from the favelas’ knows how the charges....”*

*Screenshot of a Facebook post by Marília Castro Neves, 2018*

Another Brazilian politician, Federal Deputy Alberto Fraga, spread the fake news on Twitter. After deleting the Tweet, the representative said that he had received the information by social media. He did not apologize.

<sup>11</sup> “Segundo a instituição, Marielle foi tema de 2,14 milhões de tuítes entre a noite de 14, quando ela e o motorista Anderson Gomes foram assassinados, e a meia-noite de domingo, 18 de março.”

<sup>12</sup> “Engravidou com 16 anos. Casada com Marcinho VP. Usuária de maconha. Eleita pelo Comando Vermelho e assassinada quando contrariou a bandidagem rival.”

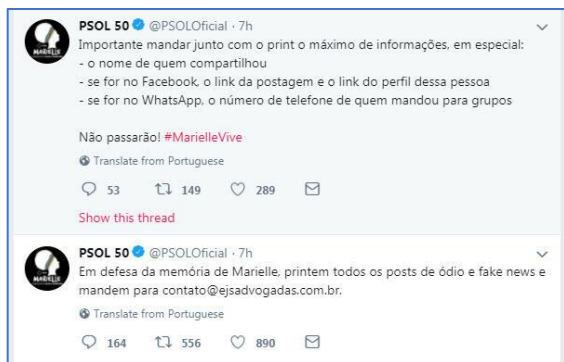
<sup>13</sup> “que leu no texto de uma amiga”



Screenshot of a Facebook post by Alberto Fraga, 2018

*“We already know the new legend on the left, Marielle Franco. She was pregnant at 16 years old, is former spouse of Marcinho VP, a marijuana user, defender of a rival faction and elected by Comando Vermelho, recently exonerated 6 of them, but who killed her, was a Public Minister.”*

The Party for Socialism and Liberty<sup>14</sup>, PSOL, is suing those who made baseless accusations against the councilwoman. In a social media post, their attorney requested that hate posts and fake news about Franco be sent to them for supporting evidence:



Screenshot of a Facebook post by PSOL official account, 2018

*Important to send with the printing and maximum of information, especially:*

- *The name of who shared*
- *If it was on Facebook, the link to the post and the link of the profile of this person*
- *If it was on WhatsApp, the telephone number of who sent it to groups*

*They shall not pass! #MarielleVive*

*In defense of the memory of Marielle, print all the hate posts and fake news and send them to contato@ejsadvogadas.com.br*

One Brazilian researcher points to the significance of her death, looking ahead toward the elections. “If anyone had any doubts that the social networks were going to be a powerful territory of dispute for narratives during the elections, the case of rumors about Marielle showed that these would be, yes, a tremendous battle ground.”<sup>15cii</sup> Another confirmed it “as a preview of how the digital environment will look during the electoral campaign in Brazil in 2018.”<sup>16 ciii</sup>

As the quality of news forgery increases, it has been complemented by increasing velocity on SM networks. “It’s becoming hard to basically say what is real and what is not... And there are also informational asymmetries. Some people may get in contact with these [fake news stories] but they

<sup>14</sup> *Partido Socialismo e Liberdade*

<sup>15</sup> *“Se alguém ainda tinha dúvidas de que as redes sociais vão ser um território de disputa fortíssima de narrativas durante as eleições, o caso dos boatos sobre Marielle mostrou que elas serão, sim, um tremendo campo de batalha”*

<sup>16</sup> *“É vista por pesquisadores como uma prévia de como poderá ser o ambiente digital durante a campanha eleitoral no Brasil em 2018.”*

might never get in contact with the information that says they are fake.”<sup>civ</sup> The gap between more convincing fake news and the fact checking that debunks them will only increase.

“And more than that, the court power is actually limited because there are forms of communication that... what can you do? Sometimes it’s encrypted communication, sometimes it’s communication between two people... And it’s very hard to understand and capture the dynamics of how this information circulates.”<sup>cv</sup>

## Response

### The Marco Civil Legislation

Brazil’s comprehensive internet law, the Marco Civil da Internet (Law 12.965), gives authority to remove online content to the Public Ministry.<sup>17</sup> This allotment of power was championed as a victory for freedom of speech and due process, since any content that is removed through the judicial process is given a public explanation for the removal.<sup>cvi</sup> In addition, it created a systematic process that took powers away from individual legislators. After Brazil’s corruption revelations in 2014 and the commencement of Operação Lava Jato, individual legislators were viewed with suspicion by the public. Frustrated politicians under suspicion of corruption sought a more expedited process for removing incriminating content.<sup>cvi</sup> Under this system, the courts have created a body of civil law that publicly outlines the justifications given for removing content. Therefore, the Marco Civil represents a comprehensive national legislation that curbs the power of the executive and legislative branches in the mediation of internet content.

This law is the long culmination of Brazil’s civil dialogue of internet governance:

*Brazil’s focus on Internet public policy issues is highly sophisticated, the product of debate within Brazilian society over how to address issues such as cybercrime, privacy, net neutrality, digital access, and spam that began in the late 1990s. This debate eventually produced a highly consultative formal process – a collaboration between the Ministry of Justice and Brazilian civil society organizations – to develop an Internet civil rights law, known as the Marco Civil da Internet.*<sup>cvi</sup>

What is more, in being so progressively oriented, the Marco Civil almost deliberately excluded any discussion of national security in its early deliberations. This is now apparent in the runup to the 2018 elections. Nonetheless, the national security apparatus has a presence on the Supreme Electoral Court fake news task force. According to Laura Tresca, head of the Digital Rights program for Brazil’s Article 19:

*“The big difference in Brazil is the participation of law enforcement. The EU’s commission is made up of academics, news organizations, social media platforms, and civil society groups. Law enforcement were not invited because there is no need to turn this into a security issue. Brazil’s federal police seek involvement because they are tasked with investigating electoral crimes. The fear is that fake news, bots, and candidates and their proxies will be ramping up their efforts in the election run up.”*<sup>cix</sup>

This background is important. No less so because future solutions to the problems of fake news and online influence operations may lie in Brazil’s robust public policy debate and the promise of new

---

<sup>17</sup> *Ministério Público*



technologies. “Brazil [continues to be] concerned with emerging Internet public policy issues, such as digital access and social inclusion on the Internet.”<sup>cx</sup> What happens in their upcoming elections, therefore, will influence the direction of other states moving forward.

### **The Securitization of Cyberspace**

There continue to be tensions between the role of individuals, governments, private business, and civic society. Cyberspace has been framed as a “strategic sector” of Brazil’s National Defense Strategy since 2008, according to CIA World Factbook. Due to the natural uncertainty of the cyber landscape and inherent dysfunction of Brazilian federal politics, Brazil has a complicated structure dividing responsibilities and prerogatives among various government sectors (see below chart).

Table 1 – Main Documents and Governmental Agencies Assigned to Deal with Cybersecurity [abridged]<sup>1</sup>

- 2008: National Defense Strategy (Law No. 6.703, 12/18/2008)
- Cyber Defense Policy (ordinance No. 3.389/MD, 12/21/2012)
- ABIN – Brazilian Agency for Intelligence
- MD – Ministry of Defense
- CD Ciber (Center for the Army for Cyber Defense)
- Presidency of the Republic
- Chamber of External Relations and National Defense (CREDEN)
- Council for National Defense (CDN)
- Department of Informational and Communication Security (DSIC)
- The Presidency’s Cabinet for Institutional Security (GSI-PR)

In a recent court ruling, “the Justice ruled for the removal, by YouTube and by Google, of videos that spread lies against the councilwoman Marielle Franco.”<sup>18 cxi</sup> This action indicates a targeted response by the court, placing the onus on private companies. It was “ruled that the businesses take down from the air, in 72 hours, 16 videos considered offensive to the honor and the memory of the councilwoman.”<sup>19 cxii</sup> Noncompliance threatens their reputation and their bottom line: “Such that they don’t complete the ruling, Google, which administers YouTube, will pay a daily fine of R\$1,000.”<sup>20 cxiii</sup>

### **What Is Being Done Ahead of the Election**

Brazilian civil society is witnessing a growing public awareness of fake news. According to a BBC poll last year of 18 nations worldwide, over 90% of Brazilians said fake news was a concern<sup>cxiv</sup>. A recent survey by Aos Fatos in Brazil, which interviewed 805 people in Rio de Janeiro, shows that 43% of the respondents usually do not rely on news coming from social media unless it is from someone they know. Over 42% of people would doubt the veracity of the news if there is a lack of citation for the source or use of provocative language.<sup>cxv</sup>

---

<sup>18</sup> “a Justiça determine a retirada, pelo Youtube e pelo Google, de videos que espalhavam mentiras contra a vereadora Marielle Franco.”

<sup>19</sup> “determinou que as empresas retirem do ar, em 72 horas, 16 videos considerados ofensivos à honra e à memória da vereadora.”

<sup>20</sup> “Caso não cumpra o prazo determinado, o Google, que administra o Youtube, pagará multa diária de R\$ 1 mil.”

The Brazilian government has also launched a series of actions in response to fake news. Brazil recently organized a joint working group between the Federal Police<sup>21</sup>, Supreme Electoral Court<sup>22</sup>, and the Public Ministry<sup>23</sup> to combat SMDIO. The group was initiated by the order of Luiz Fux, next president of the Supreme Electoral Court. Already in existence is a group presided over by the current president of the Supreme Electoral Court, though so far, the group has only produced research and findings on the influence of fake news and its promulgation through “bots.”

### **The O PL Espião (Big Spy Bill) and Legislative Responses**

Although Brazil aims to create a legal framework before the October elections, the tight legislative schedule makes that unlikely. Congress is barely functioning, the president has a popularity rating in single digits, and there is no public clamor for new legislation.<sup>cxvi</sup> In his contribution to the study of this issue, Dan Arnaudo remarks diplomatically that “the legal system has struggled to keep up with the use of computational propaganda in Brazil.”<sup>cxvii</sup>

The National Congress is considering a variety of legislative efforts designed to thwart fake news. Indeed, they have even proposed the idea of criminalizing the creation and diffusion of fake news content. Also, being considered is the imposition of heavy fines on SM platforms that fail to remove fake news content.<sup>cxviii</sup> Obviously, these considerations have renewed much of the core debate in Brazilian politics between the natural tensions in balancing free speech against libel, the transparency of judicial proceedings with the efficacy of private sector discretion.

“PL Espião would require all internet companies that wish to operate in Brazil to collect data about users, including their name, email, address, and national identity number.”<sup>cxix</sup> It is widely regarded as regressive by internet rights activists. What is more, in the historical context of Brazil as a recent dictatorship, many average citizens fear it as an abusive power-grab.

### **Alternatives to Legislation**

Brazil has a robust civil society, birthed at its transition from dictatorship three decades ago. The ITS, Institute for Technology and Society, is one of the leading non-governmental organizations that studies the issue of SMDIO closely. They publish regular analysis of SMDIO in Brazil and recently had a very successful exposition of congressional leaders who spread fake news via SM in the wake of the Franco assassination.

Additionally, citizens and NGOs are calling for a greater “soft” response from the government other than legislative ways, such as through major campaigns to increase social awareness. “The federal government ... ran major campaigns to publicize pension reform and they are doing a similar thing right now to get people to vaccinate against yellow fever...it is cheaper, faster and more effective than creating legislation,”<sup>cxx</sup> said Cristina Tardáguila, director of Agência Lupa, an independent fact checking organization set up in Rio de Janeiro.

In a large part of the studies on fake news, the conclusion is the same: above all, the education of the population is essential to combatting SMDIO. “You can’t prohibit people from lying and from sharing false stories. And many times, these people are our parents, uncles, and

---

<sup>21</sup> *Polícia Federal*

<sup>22</sup> *Tribunal Superior Eleitoral*

<sup>23</sup> *Ministério Público*

siblings, who do so inadvertently.’ says Francisco Rolfsen Belda, professor and researcher at the graduate program of media and technology at [major university] UNESP.”<sup>24</sup>

### **Outlook**

Any effective response efforts will require legislative, judicial, civil society, and even intelligence community cooperation. The more coordinated these efforts, and the better aligned their solutions, the more effective SMDIO mitigation will be. It is true that “the first studies about the impact of the phenomenon have hardly come to bare. In this context, the perspectives on the [power] of fake news and its actual effect on politics may not be as gloomy as supposed.”<sup>25cxxi</sup> However, despite the courts mobilizing to combat SMDIO, operations continue to outpace reform. At present, Brazil’s politics are too riven with conflict to present a concerted response to the issue.

---

<sup>24</sup> “Não se pode proibir as pessoas de mentir e de compartilhar coisas falsas. E muitas vezes essas pessoas são nossos pais, tios e irmãos, que fazem isso inadvertidamente”, diz Francisco Rolfsen Belda, professor e pesquisador do programa de pós-graduação de mídia e tecnologia da Unesp.”

<sup>25</sup> “Os primeiros estudos sobre o impacto do fenômeno apenas começam a vir à tona. Nesse contexto, as perspectivas sobre o poder de fogo das notícias falsas e seu efeito real na política podem não ser tão sombrias como se supunha.”

## Works Cited

---

- <sup>i</sup> Peinado, Fernando, et al. “The Distorted Online Networks of Mexico's Election Campaign.” EL PAÍS, *Síguenos En Síguenos En Twitter Síguenos En Facebook Síguenos En Twitter Síguenos En Instagram*, 22 Mar. 2018, [elpais.com/elpais/2018/03/22/inenglish/1521710735\\_571195.html](http://elpais.com/elpais/2018/03/22/inenglish/1521710735_571195.html).
- <sup>ii</sup> Soloff, Knoll. “Mexico's Troll Bots Are Threatening the Lives of Activists.” *Motherboard*, 9 Mar. 2017, [motherboard.vice.com/en\\_us/article/mg4b38/mexicos-troll-bots-are-threatening-the-lives-of-activists](http://motherboard.vice.com/en_us/article/mg4b38/mexicos-troll-bots-are-threatening-the-lives-of-activists).
- <sup>iii</sup> Noel, Andrea. “Andrea Noel (@Metabolizedjunk).” *Twitter*, Twitter, 28 Feb. 2018, [twitter.com/metabolizedjunk](https://twitter.com/metabolizedjunk).
- <sup>iv</sup> “The Twitter Rules.” *Twitter*, Twitter, [help.twitter.com/en/rules-and-policies/twitter-rules](https://help.twitter.com/en/rules-and-policies/twitter-rules).
- <sup>v</sup> Lanard, Noah, and AJ Vicens. “Facebook Is Still the Perfect Propaganda Platform. These Sketchy Mexican Pages Show Why.” *Mother Jones*, 10 Apr. 2018, [www.motherjones.com/politics/2018/04/facebook-is-still-the-perfect-propaganda-platform-these-sketchy-mexican-pages-show-why/](http://www.motherjones.com/politics/2018/04/facebook-is-still-the-perfect-propaganda-platform-these-sketchy-mexican-pages-show-why/).
- <sup>vi</sup> *Ibid.*
- <sup>vii</sup> Paraguez Kobek, Maria. “Cybersecurity in Mexico: An Overview.” *Wilson Center*, 22 Feb. 2017, doi:1 March 2018.
- <sup>viii</sup> *Ibid.*
- <sup>ix</sup> Mexico: Social Network Penetration 2017 | Statistic.” *Statista*, [www.statista.com/statistics/449869/mexico-social-network-penetration/](http://www.statista.com/statistics/449869/mexico-social-network-penetration/).
- <sup>x</sup> *Ibid.*
- <sup>xi</sup> Elfrink, Tim. “J.J. Rendon Is Latin America's Karl Rove.” *Miami New Times*, 2 Apr. 2016, [www.miaminewtimes.com/news/jj-rendon-is-latin-americas-karl-rove-6380975](http://www.miaminewtimes.com/news/jj-rendon-is-latin-americas-karl-rove-6380975).
- <sup>xii</sup> Robertson, Jordan, et al. “How to Hack an Election.” *Bloomberg.com*, *Bloomberg*, 31 Mar. 2016, [www.bloomberg.com/features/2016-how-to-hack-an-election/](http://www.bloomberg.com/features/2016-how-to-hack-an-election/).
- <sup>xiii</sup> Soloff, “Mexico's Troll Bots Are Threatening the Lives of Activists.”
- <sup>xiv</sup> Amnesty Global Insights. “Mexico's Misinformation Wars: – Amnesty Insights – Medium.” *Medium*, *Amnesty Insights*, 24 Jan. 2017, [medium.com/amnesty-insights/mexico-s-misinformation-wars-cb748ecb32e9](https://medium.com/amnesty-insights/mexico-s-misinformation-wars-cb748ecb32e9).
- <sup>xv</sup> Woody, Christopher. “McMaster: US Has Seen Signs of Russian 'Subversion and Disinformation' in Upcoming Mexican Election.” *Business Insider*, *Business Insider*, 6 Jan. 2018, [www.businessinsider.com/mcmaster-us-russia-interference-mexico-election-2018-1](http://www.businessinsider.com/mcmaster-us-russia-interference-mexico-election-2018-1).
- <sup>xvi</sup> Woody, Christopher. “McMaster: US Has Seen Signs of Russian 'Subversion and Disinformation' in Upcoming Mexican Election.” *Business Insider*, *Business Insider*, 6 Jan. 2018, [www.businessinsider.com/mcmaster-us-russia-interference-mexico-election-2018-1](http://www.businessinsider.com/mcmaster-us-russia-interference-mexico-election-2018-1).
- <sup>xvii</sup> Peinado, Fernando. “Reportaje | Diez Cosas Que Aprendí Viendo RT En Español Durante Una Semana.” EL PAÍS, *Síguenos En Síguenos En Twitter Síguenos En Facebook Síguenos En Twitter Síguenos En Instagram*, 15 Feb. 2018, [elpais.com/internacional/2018/02/12/actualidad/1518426352\\_741037.html](http://elpais.com/internacional/2018/02/12/actualidad/1518426352_741037.html).
- <sup>xviii</sup> Peinado, Fernando, et al. “The Distorted Online Networks of Mexico's Election Campaign.” EL PAÍS, *Síguenos En Síguenos En Twitter Síguenos En Facebook Síguenos En Twitter Síguenos En Instagram*, 22 Mar. 2018, [elpais.com/elpais/2018/03/22/inenglish/1521710735\\_571195.html](http://elpais.com/elpais/2018/03/22/inenglish/1521710735_571195.html).
- <sup>xix</sup> *Ibid.*
- <sup>xx</sup> Soloff, “Mexico's Troll Bots Are Threatening the Lives of Activists.”
- <sup>xxi</sup> Buendia, Jorge. “Fake Polls as Fake News: The Challenge for Mexico's Elections.” *Wilson Center*, 12 Apr. 2018, [www.wilsoncenter.org/publication/fake-polls-fake-news-the-challenge-for-mexicos-elections](http://www.wilsoncenter.org/publication/fake-polls-fake-news-the-challenge-for-mexicos-elections).
- <sup>xxii</sup> Peinado, “The Distorted Online Networks of Mexico's Election Campaign.”
- <sup>xxiii</sup> *Ibid.*
- <sup>xxiv</sup> *Ibid.*
- <sup>xxv</sup> *Ibid.*
- <sup>xxvi</sup> Amnesty Global Insights. “Mexico's Misinformation Wars: – Amnesty Insights – Medium.”
- <sup>xxvii</sup> Peinado, “The Distorted Online Networks of Mexico's Election Campaign.”
- <sup>xxviii</sup> *Ibid.*
- <sup>xxix</sup> Benton, Lloyd. “Mexico Sets Sights on Cybersecurity.” *Defence IQ*, 1 April 2018, <http://www.iqpc.com/media/1003810/51084.pdf>.
- <sup>xxx</sup> “Mexico Fights Its Own 'Fake News' Battle Ahead of Presidential Election.” *The Straits Times*, 25 Mar. 2018, [www.straitstimes.com/world/americas/mexico-fights-its-own-fake-news-battle-ahead-of-presidential-election](http://www.straitstimes.com/world/americas/mexico-fights-its-own-fake-news-battle-ahead-of-presidential-election).

- 
- xxxix Basta, Agencia. “Lanzan Campaña Contra Fake News; ‘Verificado 2018.’” *Diario Basta!*, 12 Mar. 2018, [diariobasta.com/2018/03/12/38455/](http://diariobasta.com/2018/03/12/38455/).
- xxxix “After Coming under Fire for Its Role in the 2016 U.S. Election, Facebook Inc. Is Taking Steps to Prevent What It Calls Fake News during Mexico's Presidential Campaign.” *Dallas News*, 21 Mar. 2018, [www.dallasnews.com/news/mexico-election-2018/2018/03/21/facebook-fake-news-mexico-presidential-election](http://www.dallasnews.com/news/mexico-election-2018/2018/03/21/facebook-fake-news-mexico-presidential-election).
- xxxix Soloff, “Mexico's Troll Bots Are Threatening the Lives of Activists.”
- xxxix *Ibid.*
- xxxix *Ibid.*
- xxxix *Ibid.*
- xxxix Amnesty Global Insights. “Mexico's Misinformation Wars: – Amnesty Insights – Medium.”
- xxxix “Facebook y El INE Tienen Una Relación Para La Elección Presidencial En México.” *HuffPost Mexico*, *HuffPost Mexico*, 5 Feb. 2018, [www.huffingtonpost.com.mx/2018/02/05/facebook-y-el-ine-tienen-una-relacion-para-la-eleccion-presidencial-en-mexico\\_a\\_23353523](http://www.huffingtonpost.com.mx/2018/02/05/facebook-y-el-ine-tienen-una-relacion-para-la-eleccion-presidencial-en-mexico_a_23353523).
- xxxix We Are Social. “Digital in 2018: World's Internet Users Pass the 4 Billion Mark.” *We Are Social*, 30 Jan. 2018, [wearesocial.com/blog/2018/01/global-digital-report-2018](http://wearesocial.com/blog/2018/01/global-digital-report-2018).
- xl We Are Social. “Digital in 2018 in Southern America Part 1 - North.” *LinkedIn SlideShare*, 29 Jan. 2018, [www.slideshare.net/wearesocial/digital-in-2018-in-southern-america-part-1-north-86863727](http://www.slideshare.net/wearesocial/digital-in-2018-in-southern-america-part-1-north-86863727).
- xli Caracol Radio. “Les Contamos Las Redes Sociales Que Prefieren Los Colombianos.” *Caracol Radio*, 24 Aug. 2017, [caracol.com.co/programa/2017/08/25/dos\\_y\\_punto/1503616822\\_036506.html](http://caracol.com.co/programa/2017/08/25/dos_y_punto/1503616822_036506.html).
- xlii We Are Social. “Digital in 2018 in Southern America Part 1 - North.” *LinkedIn SlideShare*, 29 Jan. 2018, [www.slideshare.net/wearesocial/digital-in-2018-in-southern-america-part-1-north-86863727](http://www.slideshare.net/wearesocial/digital-in-2018-in-southern-america-part-1-north-86863727).
- xliii El Espectador. “Caso Andrómeda y Sus Interrogantes.” *ELESPECTADOR.COM*, 4 Jan. 2018, [www.elespectador.com/noticias/judicial/caso-andromeda-y-sus-interrogantes-articulo-731765](http://www.elespectador.com/noticias/judicial/caso-andromeda-y-sus-interrogantes-articulo-731765).
- xliii Gallon, Natalie. “Guía Para Entender El Resultado Del Plebiscito En Colombia: ¿Por Qué Ganó El No?” *CNN Espanol*, Cable News Network, 2 Oct. 2016, [cnnespanol.cnn.com/2016/10/02/colombia-por-que-los-colombianos-votaron-por-el-no-en-plebiscito/](http://cnnespanol.cnn.com/2016/10/02/colombia-por-que-los-colombianos-votaron-por-el-no-en-plebiscito/).
- xliii Ramírez Prado, Julian. “El No Ha Sido La Campaña Más Barata y Más Efectiva De La Historia.” *Asuntos Legales, Noticias Legales, Financieras y Empresariales De Colombia y El Mundo.*, La Republica , 4 Oct. 2016, [www.asuntoslegales.com.co/actualidad/el-no-ha-sido-la-campana-mas-barata-y-mas-efectiva-de-la-historia-2427891](http://www.asuntoslegales.com.co/actualidad/el-no-ha-sido-la-campana-mas-barata-y-mas-efectiva-de-la-historia-2427891).
- xliii *Ibid.*
- xliii *Ibid.*
- xliii Pulzo. “El Nuevo Impuesto Que Les Cobrarían a Los Pensionados En Colombia.” *Pulzo.com*, 9 Sept. 2016, [www.pulzo.com/economia/nuevo-impuesto-pensionados-PP119241](http://www.pulzo.com/economia/nuevo-impuesto-pensionados-PP119241).
- xliii Pulzo. “Así Se Mueve El 'Cartel' De La Guerra Sucia En La Campaña De Plebiscito.” *Pulzo.com*, 20 Sept. 2016, [www.pulzo.com.co/firma-acuerdo-paz-farc/guerra-sucia-campana-plebiscito-paz-PP122976](http://www.pulzo.com.co/firma-acuerdo-paz-farc/guerra-sucia-campana-plebiscito-paz-PP122976).
- l Pulzo. “Alerta Por Mensaje Sobre Esferos Borrables Para Hacer Trampa Al Plebiscito.” *Pulzo.com*, 13 Sept. 2016, [www.pulzo.com/nacion/esferos-borrables-plebiscito-PP121795](http://www.pulzo.com/nacion/esferos-borrables-plebiscito-PP121795).
- li Bonces, Eduardo. “No Coma Cuento: Registraduría Utilizará Bolígrafos Comunes El Día De Las Elecciones.” *Www.elcolombiano.com*, 7 Feb. 2018, [www.elcolombiano.com/elecciones-2018-colombia/mentira-en-cadena-de-whatsapp-sobre-esferos-que-se-borran-con-el-calor-CD8151721](http://www.elcolombiano.com/elecciones-2018-colombia/mentira-en-cadena-de-whatsapp-sobre-esferos-que-se-borran-con-el-calor-CD8151721).
- lii Semana, Semana. “Minuto a Minuto | Así Fue La Jornada De Votación Del Plebiscito.” *Plebiscito Por La Paz Resultados De La Votación Del Plebiscito*, *Semana.com*, 2 Oct. 2016, [www.semana.com/nacion/articulo/plebiscito-por-la-paz-resultados-de-la-votacion-del-plebiscito/496455](http://www.semana.com/nacion/articulo/plebiscito-por-la-paz-resultados-de-la-votacion-del-plebiscito/496455).
- liii Petro, Gustavo. “Colombian Presidential Debate.” *Columbia por Colombia. Colombian Presidential Debate*, 23 Mar. 2018, New York, Columbia University.
- liii Matamoros, Gisela. Email Interview. 2 Apr. 2018.
- liii El Espectador. “Los Presidenciales Con Más Seguidores Falsos En Redes Sociales.” *ELESPECTADOR.COM*, 29 Jan. 2018, [www.elespectador.com/elecciones-2018/noticias/politica/los-presidenciales-con-mas-seguidores-falsos-en-redes-sociales-articulo-736152](http://www.elespectador.com/elecciones-2018/noticias/politica/los-presidenciales-con-mas-seguidores-falsos-en-redes-sociales-articulo-736152).
- liii *Ibid.*
- liii Tascón, Cecilia Orozco. “Un Oficial Del Centro Cibernético Policial De Colombia Explica Estrategia Para Elecciones.” *ELESPECTADOR.COM*, 3 Feb. 2018, [www.elespectador.com/noticias/judicial/un-oficial-del-centro-cibernetico-policial-de-colombia-explica-estrategia-para-elecciones-articulo-737056](http://www.elespectador.com/noticias/judicial/un-oficial-del-centro-cibernetico-policial-de-colombia-explica-estrategia-para-elecciones-articulo-737056).

- 
- <sup>lviii</sup> No Como Cuento, and Inteligencia Artificial Electoral 2018. “Índice De Favorabilidad Electoral De Los Candidatos Presidenciales En Redes Sociales y Medios Públicos Utilizando Inteligencia Artificial. Fecha: 11 De Marzo - 22 De Marzo De 2018. Twitter, 28 Mar. 2018, [twitter.com/NoComoCuento\\_/status/978995571422875649](https://twitter.com/NoComoCuento_/status/978995571422875649).
- <sup>lix</sup> Semana. “Me Estoy Ocupadno de Petro, Por mi Cuenta y Rieso.” *Semana*. 12 Apr, 2018. [www.semana.com/nacion/articulo/video-de-lo-que-dice-jj-rendon-sobre-duque-y-petro-entrevista-a-jaime-bayly/563483](http://www.semana.com/nacion/articulo/video-de-lo-que-dice-jj-rendon-sobre-duque-y-petro-entrevista-a-jaime-bayly/563483)
- <sup>lx</sup> Ibid.
- <sup>lxi</sup> Zuluaga, Camila. Personal Interview. 2 Apr. 2018.
- <sup>lxii</sup> Ibid.
- <sup>lxiii</sup> Voces . “¡No Coma Cuento! Venezolanos No Pueden Votar En Las Elecciones De 2018 En Colombia.” *Voces*, 2 Mar. 2018, [voces.com.co/no-coma-cuento-venezolanos-no-pueden-votar-en-las-elecciones-de-2018/](http://voces.com.co/no-coma-cuento-venezolanos-no-pueden-votar-en-las-elecciones-de-2018/).
- <sup>lxiv</sup> Ibid.
- <sup>lxv</sup> Welle, Deutsche. “Detectan Ataques Ciberneticos a Entidad Electoral De Colombia.” *MiamiDiario*, 3 Mar. 2018, [www.miamidiario.com/politica/elecciones/venezuela/colombia/juan-manuel-santos/ciberataques/elecciones-en-colombia/luis-carlos-villegas/383266](http://www.miamidiario.com/politica/elecciones/venezuela/colombia/juan-manuel-santos/ciberataques/elecciones-en-colombia/luis-carlos-villegas/383266).
- <sup>lxvi</sup> Ibid.
- <sup>lxvii</sup> Ibid.
- <sup>lxviii</sup> Pulzo. Petro publica video Manipulado en el que Duque Canta con Poncho Zuleta a “Paracos.” *Pulzo.com* 7 Apr, 2018. [www.pulzo.com/elecciones-2018/video-falso-duque-poncho-zuleta-PP466273](http://www.pulzo.com/elecciones-2018/video-falso-duque-poncho-zuleta-PP466273)
- <sup>lxix</sup> Maseri, Sergio Gómez. “Rusia Interfiere En Elecciones Colombianas: Frank Mora.” *El Tiempo*, 21 Jan. 2018, [www.eltiempo.com/mundo/eeuu-y-canada/frank-mora-afirma-que-rusia-interfiere-en-elecciones-colombianas-2018-173594](http://www.eltiempo.com/mundo/eeuu-y-canada/frank-mora-afirma-que-rusia-interfiere-en-elecciones-colombianas-2018-173594).
- <sup>lxx</sup> Ibid.
- <sup>lxxi</sup> Senate Committee on Foreign Relations. 2018. Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implication’s for U.S. National Security. U.S. Senate. Pg 38.
- <sup>lxxii</sup> Peinado, Fernando. 2018, Feb 15. Diez cosas que aprendí viendo RT en Español durante una semana. El Pais. [https://elpais.com/internacional/2018/02/12/actualidad/1518426352\\_741037.html](https://elpais.com/internacional/2018/02/12/actualidad/1518426352_741037.html)
- <sup>lxxiii</sup> Henao, Diana Rincón. “¿Qué Tanto Influyen Las Redes Sociales Con El Voto Real En Colombia?” *El Tiempo*, 8 Mar. 2018, [www.eltiempo.com/elecciones-colombia-2018/jurados-y-votantes/influencia-de-las-redes-sociales-en-el-voto-real-en-colombia-191332](http://www.eltiempo.com/elecciones-colombia-2018/jurados-y-votantes/influencia-de-las-redes-sociales-en-el-voto-real-en-colombia-191332).
- <sup>lxxiv</sup> Ibid.
- <sup>lxxv</sup> El Espectador. “Candidata Uribista Comparte Falsas Imágenes De Atentado Del Eln y Policía La Desmiente.” *ELESPECTADOR.COM*, 9 Feb. 2018, [www.elespectador.com/noticias/politica/candidata-uribista-comparte-falsas-imagenes-de-atentado-del-eln-y-policia-la-desmiente-articulo-738297](http://www.elespectador.com/noticias/politica/candidata-uribista-comparte-falsas-imagenes-de-atentado-del-eln-y-policia-la-desmiente-articulo-738297).
- <sup>lxxvi</sup> El Herald. “Santos Alerta Sobre Posibles 'Ciberataques' Durante Las Elecciones De 2018.” *El Herald*, 22 Jan. 2018, [www.elheraldo.co/politica/santos-alerta-sobre-posibles-ciberataques-durante-las-elecciones-de-2018-450540](http://www.elheraldo.co/politica/santos-alerta-sobre-posibles-ciberataques-durante-las-elecciones-de-2018-450540).
- <sup>lxxvii</sup> Welle, Deutsche. “Detectan Ataques Ciberneticos a Entidad Electoral De Colombia.” *MiamiDiario*, 3 Mar. 2018, [www.miamidiario.com/politica/elecciones/venezuela/colombia/juan-manuel-santos/ciberataques/elecciones-en-colombia/luis-carlos-villegas/383266](http://www.miamidiario.com/politica/elecciones/venezuela/colombia/juan-manuel-santos/ciberataques/elecciones-en-colombia/luis-carlos-villegas/383266)
- <sup>lxxviii</sup> Restrepo, Margarita. “Proyecto De Ley 224 De 2017. » Margarita Restrepo.” *Margarita Restrepo Website*, 20 May 2017, [margaritarestrepo.com/2017/05/proyecto-de-ley-224-de-2017.html](http://margaritarestrepo.com/2017/05/proyecto-de-ley-224-de-2017.html).
- <sup>lxxix</sup> CIA World Factbook. Available online: <https://www.cia.gov/library/publications/the-world-factbook/geos/br.html>
- <sup>lxxx</sup> Ibid.
- <sup>lxxxi</sup> Gordon, Kyle. “Topic: Internet Usage in Brazil.” [www.statista.com](http://www.statista.com), [www.statista.com/topics/2045/internet-usage-in-brazil/](http://www.statista.com/topics/2045/internet-usage-in-brazil/).
- <sup>lxxxii</sup> Mares, David & Trinkunas, Harold. Aspirational Power. Brazil on the Long Road to Global Influence. Brookings Institution Press. p 154.
- <sup>lxxxiii</sup> Hootsuite Media Inc. “Digital in 2018.” Hootsuite, 2018, [hootsuite.com/pages/digital-in-2018](http://hootsuite.com/pages/digital-in-2018).
- <sup>lxxxiv</sup> Ibid. Page 9.
- <sup>lxxxv</sup> Arnaudo, Dan. “Computational Propaganda in Brazil: Social Bots During Elections” (Working Paper No. 2017.8). Computational Propaganda Research Project. University of Oxford. Page 9
- <sup>lxxxvi</sup> Arnaudo. Page 14.
- <sup>lxxxvii</sup> Ibid.
- <sup>lxxxviii</sup> “A 9 Meses Da Eleição, TSE Quer Combater Notícias Falsas - Eleições 2014 No G1 – Vídeos, Pesquisas, Apuração De Votos e Resultados - Catálogo De Vídeos.” Eleições 2014 No G1 – Vídeos, Pesquisas, Apuração De

---

Votos e Resultados, 19 Jan. 2018, [g1.globo.com/politica/eleicoes/2014/videos/t/todos-os-videos/v/a-9-meses-da-eleicao-tse-quer-combater-noticias-falsas/6434567/](http://g1.globo.com/politica/eleicoes/2014/videos/t/todos-os-videos/v/a-9-meses-da-eleicao-tse-quer-combater-noticias-falsas/6434567/).

<sup>lxxxix</sup> Nalon, Tai, 02/19/1028 Interview

<sup>xc</sup> Ibid.

<sup>xc</sup> Ibid.

<sup>xcii</sup> “Brazil Mainstream Media Admits Spreading Fake News About Lula.” News | TeleSUR English, TeleSUR, 23 May 2017, [www.telesurtv.net/english/news/Brazil-Mainstream-Media-Admits-Spreading-Fake-News-About-Lula-20170523-0025.html](http://www.telesurtv.net/english/news/Brazil-Mainstream-Media-Admits-Spreading-Fake-News-About-Lula-20170523-0025.html).

<sup>xciii</sup> Bergamasco, Bronzatto & Gonçalves. “A ameaça das ‘fake news’” “*The Threat of Fake News*”

<sup>xciv</sup> Ibid.

<sup>xcv</sup> Ibid.

<sup>xcvi</sup> Ibid.

<sup>xcvii</sup> Gragnani, Juliana. “Como combate a mentiras sobre Marielle superou racha ideológico e pode antecipar guerra eleitoral nas redes” How Combatting lies about Marielle Overcame the Ideological Split and Anticipates the Electoral War in Social Networks” BBC Português. 03/27/2018. Available online:

<http://www.bbc.com/portuguese/brasil-43549550?SThisFB>

<sup>xcviii</sup> Wagner, Beatriz. “O assassinato duplo de Marielle Franco: depois do corpp, o caráter.” “The double assassination of Marielle Franco: After her body, her character” Radioagência Nacional. 03/18/2018. Available online: <https://www.sbs.com.au/yourlanguage/portuguese/en/audiotrack/o-assassinato-duplo-de-marielle-franco-depois-do-corpo-o-carater>

<sup>xcix</sup> Affonso, Carlos. “Marielle e os porta-vozes da desinformação” 03/20/2018. Tecfront. Available online:

<https://tecfront.blogosfera.uol.com.br/2018/03/20/marielle-e-os-porta-vozes-da-desinformacao/>

<sup>c</sup> Veja staff. “Desembargadora diz que Marielle ‘estava engajada com bandidos’” “Judge says that Marielle ‘was engaged with criminals’”. Veja. 03/19/2018. Available online: <https://veja.abril.com.br/brasil/desembargadora-diz-que-marielle-estava-engajada-com-bandidos/>

<sup>ci</sup> Ibid.

<sup>cii</sup> Gragnani. “Como combate a mentiras sobre Marielle superou racha ideológico e pode antecipar guerra eleitoral nas redes” How Combatting lies about Marielle Overcame the Ideological Split and Anticipates the Electoral War in Social Networks”

<sup>ciii</sup> Ibid.

<sup>civ</sup> 04/11/2018 Interview with Professor Ronaldo Lemos

<sup>cv</sup> Ibid.

<sup>cvi</sup> Lemos, Ronaldo, 01/31/2018 Interview.

<sup>cvi</sup> Ibid.

<sup>cvi</sup> Mares, David R., and Harold A. Trinkunas. *Aspirational Power: Brazil on the Long Road to Global Influence*. Brookings Institution Press, 2016. p. 154

<sup>cix</sup> Downie, Andrew. “Ahead of elections, Brazil's police announce plan to crackdown on 'fake news'” The Committee to Protect Journalists. 01/30/2018. Available online: <https://cpj.org/blog/2018/01/ahead-of-elections-brazils-police-announce-plan-to.php>

<sup>cx</sup> Mares & Trinkunas, page 154.

<sup>cx</sup> PSOL50. “Justiça determina que Youtube e Google retirem do ar 16 vídeos caluniosos contra Marielle” “Justice Rules that Youtube and Google Take Down 16 Calumnious Videos Against Marielle” 03/23/2018. Available online: <http://www.psol50.org.br/justica-determina-que-youtube-e-google- retirem-do-ar-16-videos-caluniosos- contra-marielle/>

<sup>cxii</sup> Ibid.

<sup>cxiii</sup> Ibid.

<sup>cxiv</sup> Downie. “Ahead of elections, Brazil's police announce plan to crackdown on 'fake news'”

<sup>cxv</sup> Spagnuolo, Sérgio. “Leitores Desconfiam De Notícias Recebidas Por WhatsApp, Mas Não Checam Informações.” Aos Fatos, Aos Fatos, 14 Mar. 2018, [aosfatos.org/noticias/leitores-desconfiam-de-noticias-recebidas-por-whatsapp-mas-nao-checam-informacoes/](http://aosfatos.org/noticias/leitores-desconfiam-de-noticias-recebidas-por-whatsapp-mas-nao-checam-informacoes/)

<sup>cxvi</sup> Ibid.

<sup>cxvii</sup> Arnaudo. Page 26.

<sup>cxviii</sup> Valente, Jonas. “PF, TSE e Ministério Público vão criar grupo para combater fake news na eleição” Agência Brasil. 01/04/2018. Available online: <http://agenciabrasil.ebc.com.br/politica/noticia/2018-01/pf-tse-e-ministerio-publico-va-criar-grupo-para-combater-fake-news-na>

<sup>cxix</sup> Arnaudo. Page 26.

---

<sup>cxx</sup> Downie. “Ahead of elections, Brazil's police announce plan to crackdown on 'fake news'”  
<sup>cxxi</sup> Ibid.