KAUTILYA
SCHOOL OF
PUBLIC POLICY

# CAPSTONE PROJECT

**Role of Open-Source Intelligence in Electoral Analysis and Outcomes –A Policy Perspective**

**Capstone Project Number: CP-2025-03**

Submitted by: Mr Siddharth Rao (MPP Cohort: 2023-25)

Under the Supervision of: Dr. Vishnu S. Pillai, Assistant Professor at Kautilya School of Public Policy

***Cite this Report*** *as Rao, S. (2025). Role of Open-Source Intelligence in Electoral Analysis and Outcomes –A Policy Perspective. Kautilya School of Public Policy [online]. Available at: https://kspp.edu.in//capstone-project/role-of-open-source-intelligence-in-electoral-analysis-and-outcomes-a-policy Perspective*

# Role of Open-Source Intelligence in Electoral Analysis and Outcomes – A Policy Perspective

**Submitted to Kautilya School of Public Policy in Partial Fulfillment of the Requirement for the Degree of Master of Public Policy (MPP)**

**2023-25**

**Siddharth Rao, 2023004769**

**Under the Supervision of**

**Dr. Vishnu Pillai**

**Assistant Professor**


**Kautilya School of Public Policy,**

**Gandhi Institute of Technology and Management**

**(Deemed to be University)**

**Rudraram, Telangana 502329**

**SELF-DECLARATION**

This is to certify that the thesis titled ***Role of Open Source Intelligence in Electoral Analysis and Outcomes - A Policy Perspective*** is my original work and has not previously formed the basis for the award of any Degree, Diploma, Associateship or Fellowship to this or any other University.

**Siddharth Rao**

**April 07, 2025**

## ACKNOWLEDGEMENTS

I am deeply grateful to my professor, Dr. Vishnu Pillai, whose constant support, insightful feedback, and patient guidance have shaped this capstone from inception to completion. His academic rigor and mentorship have been invaluable throughout this research journey.

I extend my heartfelt appreciation to my father, whose profound political wisdom and teachings have significantly informed my psephological understanding. His expert insights and encouragement were indispensable in nurturing my passion for political analysis.

A special thanks to my fellow coursemates in the Master of Public Policy (MPP) program, whose camaraderie, stimulating discussions, and collaborative spirit enriched my academic journey immensely. Their collective enthusiasm and intellectual curiosity made the learning experience memorable and enlightening.

Lastly, I would like to acknowledge Mr. Bharat Bhushan and Mr. Sreepad Nandan at Absolute Politico, whose generous support and encouragement provided me with the critical resources and practical insights necessary to realize this research. Their professional guidance was instrumental in enhancing the relevance and depth of my study.

Thank you all for contributing meaningfully to this significant milestone in my academic and personal growth.

## Table of Contents

## Executive Summary

Over the last decade, as India rapidly digitized, so did its democratic processes and with the proliferation of social media, as it happened, the influence of Open Source Intelligence (OSINT) (in simpler terms, openly available information whether in the form of social media posts or government reports or media publications) has become powerful and also problematic. This capstone attempts to explore how OSINT - including social media and AI-driven information campaigns, influencer marketing, and data analytics have reshaped political campaigns, influencing voter engagement and democratic discourse in the 2014, 2019, and 2024 general elections.

OSINT is a double-edged sword, as on the one hand, it enhances campaign strategies, by enabling real-time sentiment analysis, precise targeting, participatory outreach, and essentially creates a level playing ground for small and big political entities alike. However, it also opens the pandora's box of misinformation, deepfakes, coordinated disinformation, and algorithmic bias. This study aims to reveal the vulnerabilities in India's electoral ecosystem as far as OSINT is concerned, via studying examples like bot-driven campaigns, deepfakes in regional elections, and more.

This capstone also argues for the necessity of a regulatory architecture that goes beyond diagnosing the problem as there is an urgent need for policy intervention. An architecture that can maintain its pace with evolving technologies, encompassing transparent political advertising rules, safeguards against manufactured information, and accountability for digital influencers apart from AI-aided monitoring systems for oversight mechanisms, is critical in today's electoral context.

OSINT is here to stay, and that is why, there is a necessity to bridge the gap between technological disruption and democratic resilience.

## INTRODUCTION

Long before social media transformed smartphones into political tools, open-source information had already proven itself as a formidable instrument of influence. In the early 20th century, Adolf Hitler's regime utilized emerging media technologies to spread propaganda, including mass-produced phonograph recordings of his speeches, which were amplified through speakers mounted on trucks and broadcast across cities (Herf, 2006). These were accompanied by posters, films, and newspapers—openly distributed materials aimed at shaping public perception on a national scale.

Even earlier, the suffragette movement in the UK and the US mastered the use of public space and print media to drive change. Activists plastered cities with powerful visuals, pamphlets, and slogans—an early form of what we might now consider open-source messaging—leveraging visibility to influence public debate and policymaking (Crawford, 2003; Tickner, 1988).

These examples remind us that open source information—whether visual, auditory, or textual—has always played a pivotal role in the choreography of power. The only thing that has changed is the velocity and scale at which this influence now operates.

Fast forward to 21st-century India, and the same dynamics have taken on digital lives of their own. Open Source Intelligence (OSINT)—the practice of gathering actionable insights from publicly available information—has become an indispensable tool in modern electoral strategy. Unlike traditional espionage or political canvassing, OSINT thrives on platforms like WhatsApp, Twitter (now X), Facebook, and YouTube, where user-generated content, metadata, and sentiment trails form the building blocks of campaign narratives and voter targeting.

India's 2014 general elections marked a turning point in this technological evolution. For thefirst time, a major political party—the Bharatiya Janata Party (BJP)—employed data analytics, WhatsApp mobilization, and volunteer networks to strategically target voters, amplify narratives, and reshape digital discourse (Chakravartty & Roy, 2017). This utilization of OSINT redefined electoral campaigning in the country, apart from helping the BJP secure a majority.

The same ecosystem matured by 2019 and also took a dark turn, with deepfake technologies, bot networks, trend-manipulation tactics, and other such methods entering the fray and this blurred the line between persuasion and manipulation (Jakesch et al., 2021; Ferrara et al., 2016). A major tool for information dissemination and misinformation as well turned out to be WhatsApp, as political parties sought to create up to three WhatsApp groups for each of the 927,533 polling booths in the country (Aneez et al., 2019). In 2024, tools became more sophisticated with generative AI becoming accessible to everyone, and this pushed the takes higher as AI and synthetic media started being employed to manufacture persuasive political content (Christopher, 2024; Ghosh, 2024).

Today, the challenge is not just in how OSINT is used but how there is no tangible way to regulate it. India is a democracy with over 600 million digitally equipped citizens (TRAI, 2023). Implying that 600 million people can be influenced digitally, by algorithms, private platforms, and political operatives that own and operate the infrastructure of influence. Also, OSINT democratises information dissemination as well, because anyone with digital access can put out information online.

This study aims to examine the double-edged sword that OSINT is in Indian electoral politics, with its potential to empower participatory engagement and its propensity do distort

democratic processes. To explore this, the research is organized into eight interlinked chapters, each building on a distinct aspect of the OSINT landscape:

- Chapter 1 introduces the idea of computational propaganda and discusses the transformative impact it had on Indian elections.
- Chapter 2 delves into social media manipulation, hashtag engineering, disinformation, coordinated misinformation, and more.
- Chapter 3 explores hybrid campaigning, where traditional voter outreach is combined with digital microtargeting and AI-driven voter segmentation.
- Chapter 4 analyzes the deepfake phenomenon, documenting how synthetic media has been deployed in Indian elections to distort political speech and discredit opponents, and also on the legitimate use of deepfakes
- Chapter 5 evaluates the resilience of India's electoral infrastructure, including systemic vulnerabilities like the First-Past-The-Post system, gerrymandering, and OSINT-based voter profiling.
- Chapter 6 examines the rising power of influencer-based political advertising, where paid political content is disguised as organic opinion, bypassing electoral oversight.
- Chapter 7 reflects on the role of algorithms and AI, highlighting the lack of transparency in recommendation systems and the broader implications for electoral fairness.
- Chapter 8 focuses on cross-platform coordination, where multiple platforms are used in conjunction with each other, making it harder to regulate.

# RESEARCH METHODOLOGY

Adopting a qualitative research approach, this study combines comprehensive secondary data analysis and semi-structured expert interviews that were thematically analysed. The goal of this methodology to capture the evolving and nuanced landscape of Open Source Intelligence (OSINT) in the Indian electoral context.

## Data Analysis

Existing academic research, institutional reports, journalistic sources and documented publicly available case studies were used for the Chapters 2-8, with the following systematic steps:

1: Structured keyword searches were conducted on databases and sources like JSTOR, ResearchGate, Election Commission of India, etc; by using keywords like “social media manipulation”, “deepfakes”, “AI in electoral campaigns”, “OSINT in elections”, “computational propaganda in elections”, relevant to Indian elections.

2: Content filtering was done with a focus on credibility of sources, like considering only peer-reviewed journals, reputable think-tanks and media outlets, etc, with additional focus on sources that explicitly spoke about 2014, 2019, and 2024 Indian general elections; regarding OSINT factors like digital manipulation and digital propaganda.

3: The information was categorised thematically addressing various OSINT phenomena like:

- Chapter 2: Social media manipulation
- Chapter 3: Hybrid campaigning
- Chapter 4: Deepfake misinformation

- Chapter 5: Electoral system resilience
- Chapter 6: Influencer political advertising
- Chapter 7: Algorithmic influence and AI
- Chapter 8: Cross-platform coordination

4: The data from secondary sources was analysed thematically and organised into chapters as listed above, with distinct patterns, common phenomena, and emerging trends taken into consideration. Comparative analysis across 2014, 2019, and 2024, elections illustrated technological and strategic evolutions of campaigns and their impact on democratic processes.

5: Cross-verification of topics was done to ensure validity and reliability. Examples of topics triangulated include the spread of misinformation via WhatsApp (Aneez et al., 2019; Bradshaw & Howard, 2018), documented cases of political deepfakes (Ghosh, 2024; Christopher, 2024), and analyses of hybrid campaigning strategies (Chadwick, 2017; Chakravartty & Roy, 2015).

6: The insights were then integrated into a logically structured, cohesive narrative for each thematic chapter, with emphasis on the implications and challenges that OSINT brings in to India's electoral context.

**Qualitative Interviews**

Five semi-structured, qualitative interviews were performed with the participants having expertise in social media strategy, OSINT, and digital electoral campaigning. Virtual interviews were conducted, with consented audio-recording and transcription. Confidentiality

was also prioritised, with strict adherence to ethical research standards to ensure privacy and informed participations.

The interview data was analysed thematically, with an emphasis on practical applications of OSINT in electoral contexts, ethical considerations, regulatory gaps, and other perspectives on digital electoral practices.

**Methodological Limitations**

The study acknowledges limitations such as potential biases from purposive sampling, limited generalizability of interview findings, and subjectivity inherent in qualitative interpretation.

**Conclusion**

This methodology combined secondary data analysis and qualitative insights to gain a comprehensive understanding of OSINT's role in electoral processes, acknowledging limitations while attempting to maintain analytical rigour and validity.

# 1: Computational Propaganda in Indian Elections

Computational propaganda is essentially the strategic use of automated digital tools including AI and social media algorithms to shape and manipulate public opinion and it has transformed electioneering worldwide (Woolley & Howard, 2016). In India, the world's largest democracy, where over 600 million internet users provide a vast audience for digital political operations (Aneez et al., 2019), this shift is very visible and pronounced.

As social media started increasingly dominating political discourse, it is natural for India to become a testing ground for sophisticated propaganda strategies, often orchestrated by political parties, private firms, and ideologically driven groups. The 2014 and 2019 general elections demonstrated how digital tools could mobilize voters, shape narratives, and at times, manipulate electoral processes (Bradshaw & Howard, 2018).

This chapter examines how computational propaganda functions in Indian elections, exploring key mechanisms, case studies, and its impact on democratic integrity.

## 1.1: The Rise of Computational Propaganda in India

There has been a significant evolution of India's digital electioneering in the past decade. Traditional media as a primary source of political information has been overshadowed by platforms like WhatsApp, Facebook, Twitter, and Youtube (Aneez et al., 2019). With high smartphone penetration and affordable data plans, political campaigns have increasingly relied on algorithm-driven content dissemination to influence public opinion.

India saw the first large-scale deployment of social media-driven campaigns in the 2014 elections, with the BJP effectively utilizing WhatsApp and Facebook, with live events, and micro-targeted ads (Jakesch et al., 2021). However, by 2019, the game changed drastically as the 2019 elections were essentially a full-scale digital war. Automated

disinformation, cross-platform propaganda, bot and troll driven engagement became common (Bradshaw & Howard, 2018).

### 1.2: Key Mechanisms of Computational Propaganda

Computational propaganda is a multi-layered and highly adaptive phenomenon in Indian elections, combining technology with human coordination. The following are the primary mechanisms:

1. Automated Bots and Fake Accounts

Bots on social media are used as a part of political campaigns to simulate engagement, drown out dissenting voices, and to manufacture consent. They can also artificially inflate trends on Twitter, boost reach, and retweet political messaging. This can be done either by automated bots or by fake accounts (Ferrara et al., 2016).

- A study found that 19% of political tweets in India during the 2019 elections were generated by bot networks (Jakesch et al., 2021).
- BJP’s "Main Bhi Chowkidar" campaign amassed over 1 million tweets in 48 hours, with significant bot-driven amplification.

Bots can also be used to mass-report opposition accounts and handles, causing the accounts to be suspended or to have reduced visibility.

2. Cross-Platform Coordination: The WhatsApp-Twitter Pipeline

Using closed networks like WhatsApp to coordinate mass engagement on open platforms like Twitter and Facebook is a sophisticated OSINT tactic for political campaigning (Jakesch et al., 2021).

- Party operatives distribute pre-composed tweets, meme templates, viral slogans, and any other propaganda material on WhatsApp groups and volunteers on these groups post en masse.
- By 2019, BJP had over 900,000 WhatsApp groups, providing real-time coordination for trending topics (Aneez et al., 2019). Via groups like these, parties can coordinate hashtag campaigns, which are amplified by volunteers and bots, ensuring their visibility in mainstream media coverage.

The intriguing point here is that there is an illusion of organic public discourse, as these posts essentially seem organic, giving credibility to manipulative narratives.

3. Misinformation and Deepfake Technology

Deepfake technology is a potent disinformation tool in Indian elections as it enables AI-driven misinformation (Howard et al., 2020). There have been deepfakes where one party leader was endorsing their opposition but apart from that, there is also a legitimate use of deep-fakes as AI-generated speech models have been used to synthesize campaign messages in multiple regional languages, enhancing reach while evading fact-checking mechanisms.

The combination of synthetic media and deepfakes has blurred the line between what real political discourse is versus fabricated narratives and this makes it difficult for voters to differentiate truth from falsehood.

## Chapter 2: Social Media Manipulation in Indian Elections

With over 600 million internet users in India, there has been an extensive rise in social media manipulation - using social media strategically to influence public opinion through misinformation, coordinated campaigns, and automated amplification. Platforms like Facebook, WhatsApp, Twitter (now X), and YouTube have become central to political discourse (Aneez et al., 2019).

These platforms offer unprecedented access to voters and enable large-scale manipulation by ideological groups and political actors, as evidenced in the 2014, 2019, and 2024 Indian general elections; all of which have seen increasing levels of social media manipulation including bot-driven campaigns and AI-generated disinformation and misinformation.

### 2.1: 2014 General Elections: The Digital Campaign Emergence

The 2014 general elections marked the beginning of large-scale digital campaigning in India (Pal et al., 2019) and social media became a key battleground, as parties could use it to communicate directly with targeted voters, while bypassing traditional media and the oversight mechanisms that exist for traditional media.

#### *BJP's Digital Strategy and the WhatsApp Revolution*

- Mass Mobilization: The BJP pioneered mass social media mobilization, referred to in common media as the BJP IT cell, which is essentially a vast network of social media volunteers who amplify pro-party narratives and messaging on Facebook and Twitter (Chakravartty & Roy, 2015). Pushing hashtags, engaging in debates and discourses, attacking opposition narratives and figures have been the activities of this digital

army, and a side effect of this is creating an impression of widespread grassroots support.

- Microtargeting: BJP was the first Indian party to use data analytics and psychographic profiling to customize political advertisements on Facebook (Aneez et al., 2019).
- WhatsApp Networks: Thousands of coordinated WhatsApp groups also aid in political messaging across constituencies (Pal et al., 2019).

Employing a digital-first strategy enabled the BJP to dominate the online narrative and this was also the time when "Ab Ki Baar Modi Sarkaar" was a battle-cry that echoed across platforms. Eventually the party secured a landslide victory, securing 282 out of 543 seats in the 2014 elections.

### 2.2: 2019 General Elections: The Rise of Misinformation and Coordinated Trends

While the 2014 elections saw the emergence of social media manipulation, 2019 elections witnessed a dramatic increase in the same, particularly on WhatsApp, Twitter, and Facebook (Jakesch et al., 2021).

#### *WhatsApp as a Political Weapon*

- Fake News Epidemic: With fabricated messages, edited videos, deepfake audio clips, and other such constructed messaging, WhatsApp became a primary source of misinformation, and the messaging was circulated among millions of users (Howard, 2020).
- Automated Messaging: BJP aimed to create three WhatsApp groups for each of India's 927,533 polling booths, potentially reaching 700 million people (Chaturvedi, 2019). This could enable precise micro-targeting.

### *Case Study: Twitter Trend Manipulation*

Automated bots and paid influencers started being used by political parties extensively to create an artificial trending of hashtags (Jakesch et al., 2021). Research found that:

- Bot accounts generated 19% of tweets related to Indian elections (Ferrara et al., 2019).
- BJP's "Main Bhi Chowkidar" campaign amassed 1 million tweets in 48 hours, and there was evidence of bot-driven amplification (Jakesch et al., 2021).
- Congress-affiliated groups employed similar tactics and amplified hashtags that were critical of BJP leaders (Howard, 2020).

Twitter proved itself as a formidable platform for shaping political discourse in the 2019 elections, whether through authentic or inauthentic engagement.

**2.3: 2024 General Elections: AI, Deepfakes, and Hybrid Campaigning**

With the experiences of the earlier two elections in conjunction with the advancements in AI, generative LLMs and deepfakes, there has been a significant evolution in social media being used for political propaganda.

### *Deepfake Technology in Political Campaigns*

- AI-Generated Videos: Politicians and their opponents used deepfakes to fabricate speeches, endorsements, and controversies (Christopher, 2024).
- AI-Powered Microtargeting: Political campaigns used AI-generated avatars to interact with voters in regional languages, personalizing their outreach efforts (Ghosh, 2024).

### *Case Study: Misleading Deepfake Video of Amit Shah*

In April 2024, there was a deepfake video which falsely depicted BJP leader Amit Shah announcing the removal of caste-based reservations (BBC News, 2024). Before it was eventually debunked by independent fact-checkers, it was widely circulated on Facebook and Whatsapp, reaching millions of social media users. This demonstrated how deepfakes can manipulate public perception.

- The video was circulated widely on Facebook and WhatsApp before being debunked by independent fact-checkers.
- Despite fact-checking, the video had already reached millions of voters, showcasing how deepfakes can manipulate public perception (Christopher, 2024).

AI-driven propaganda became one of the biggest challenges of the 2024 elections, bringing to light the challenges posed by it, making regulation and detection tools an imperative.

### 2.4: Impact on Democratic Processes

There have been significant consequences of the widespread use of social media manipulation in elections:

- Erosion of Trust in Media: Misinformation campaigns have resulted in reduced trust in mainstream and digital media sources (Bradshaw & Howard, 2018).
- Increased Political Polarization: Content personalization because of algorithm-driven nature of social media platforms has resulted in deepening the ideological divide among voters (Tucker et al., 2018).

- Threats to Election Integrity: There is now a blur between truth and fiction owing to AI-powered disinformation campaigns. This has made informed choice difficult for voters (Howard, 2020).

---

## Chapter 3: Hybrid Campaigning in Indian Elections

Hybrid campaigning in contemporary electoral politics refers to the strategic integration of traditional on-field methods of campaigning with digital outreach strategies and now, it has become a defining feature of electioneering (Chadwick, 2017). Enabling political entities to blend in-person engagement with digital communication results in maximised reach and enhanced voter engagement.

As India has a vastly diverse electorate with about 50% digital penetration and multilingual demographic, is a unique case for hybrid campaigning. While early Indian elections relied on public rallies and door-to-door canvassing, it has now evolved to include sophisticated methods like AI-powered data analytics and social media warfare, demonstrating the profound transformation that has taken place in political communication(Rao, 2020). This chapter examines the evolution and implementation of hybrid campaigning across the 2014, 2019, and 2024 general elections, providing a comparative analysis of campaign strategies.

### 3.1: 2014 General Elections: The Digital Emergence

In 2014, as discussed earlier, it was a watershed moment in digital campaigning as the BJP pioneered integrating social media outreach with traditional campaigning. Prior to this, Indian elections relied on rallies, roadshows, television and radio appearances but BJP's 2014 campaign revolutionized electioneering by employing social media and data analytics with a volunteer-driven digital movement apart from on-ground campaigning (Pal et al., 2016).

### *BJP's Integrated Campaign Strategy*

1. Traditional Rallies and Events
    - BJP mobilized large-scale rallies, utilizing Narendra Modi's charismatic appeal to attract mass participation.
    - Parallel to this, door-to-door outreach and grassroots mobilization of party cadre and other influential figures helped reinforce the party's messaging (Mahapatra, 2015).

2. Digital Amplification
    - To ensure the campaign reaches audiences beyond those who physically attended the rallies, Facebook, Twitter, and YouTube were used to broadcast Modi's rally speeches.
    - WhatsApp groups were extensively used for micro-targeting voters in different constituencies.

3. Innovative Initiatives: India272+
    - The India272+ app launched by the BJP and the subsequent interactive volunteer campaign enabled active engagement online and offline (Jaffrelot, 2015).
    - Mobilizing urban youth and first-time voters, this hybrid strategy mobilized made political engagement more participatory (Singh, 2016).

**3.2: Impact:**

Political commentators have attributed BJP's 2014 win to this innovative hybrid model, proving the efficacy of blending on-ground campaigning with OSINT-enabled digital outreach (Chaturvedi, 2019).

### 3.3: 2019 General Elections: The Digital Surge

Digital platforms evolved by 2019, becoming potent political tools to have real-time voter engagement and data-analytics driven social media strategies. By 2019, Congress also recognized the need for a comprehensive hybrid strategy, to leverage social media influence alongside on-ground presence (Rao, 2020).

### 3.4: Congress Party's Digital Engagement

1. Enhanced Social Media Presence
    - The Indian National Congress started actively engaging on Twitter and Facebook, to counter the BJP's dominance in the digital space by 2019 elections.
    - The party focused on a youth-oriented digital campaign, targeting first-time voters and urban professionals (Singh, 2021).
2. Integration with Ground Campaigns
    - Synchronizing social media narratives with on-the-ground events, Congress initiated a cohesive hybrid strategy (Nair, 2019).
    - Offline, on-ground rallies were livestreamed and content from these rallies was promoted on WhatsApp and other platforms, apart from complementing the strategy via AI-driven chatbots (Aneez, Neyazi, & Ranganathan, 2020).

## *Case Study: Poonam Mahajan's Youth-Centric Campaign*

Contesting from Mumbai North Central, BJP's Poonam Mahajan, took to an extremely innovative youth-centric hybrid campaign.

- #PoonamPhirSe Campaign:

    - Instagram and Snapchat were used in the campaign to create memes, interactive posts and polls, and to leverage influencers for campaigning (Ravi, 2019).
    - There were pop-culture references that millennials and Gen Z can relate to, in the political messaging of the #PoonamPhirSe campaign (Tripathi, 2020).

- **Merchandise and Gamification:**
    - The elections also saw customized campaign merchandise like T-Shirts and mobile accessories, with political messaging in youth-centric formats.
    - Volunteers were incentivised with gamification techniques like digital badges and shoutouts (Verma, 2019).

Hybrid campaigning with a digital-first strategy was established as the key to electoral success, post 2019 elections.

### 3.5: 2024 General Elections: The AI and Data Analytics Era

There was a paradigm shift within the hybrid campaigning ecosystem by 2024 elections as Artificial Intelligence - generative and predictive came into play, along with diverse sources for getting hyper-personalised voter outreach becoming integral components of electoral strategies (Singh, 2024). AI-driven messaging, predictive data analytics, chatbot interactions, and big-data insights were embraced by political parties.

### 3.6: BJP's Technological Advancements

1. AI-Powered Voter Outreach
    - AI-driven tools analyzed voter sentiment and behavioral patterns, enabling personalized messages tailored to individual concerns (Ganguly, 2023).
    - Chatbots on WhatsApp provided real-time campaign updates and issue-based discussions, facilitating direct communication with voters (Sengupta, 2023).

2. Enhanced Ground Mobilization
    - Data analytics were used to optimize rally locations, ensuring targeted engagement in critical constituencies (Sharma, 2024).
    - Political parties also used AI-driven geo-fencing technology to send personalized push notifications to voters who attended rallies (Chaudhuri, 2023).

# Chapter 4: Deepfake Misinformation in Indian Elections

Deepfake technology has brought in both opportunities and threats, blurring the line between fact and fiction, as political actors can fabricate reality with an unprecedented level of accuracy. AI generated videos, audios, and images started off as experimental entertainment technology but they have now become a potent weapon in the hands of political powers to influence electoral processes and electorate perceptions in a country with 600 million internet users. Owing to the open-nature of these technologies, it can be argued that deepfake technologies can pose a threat to democracy, as they offer a convenient way to shape political discourse and invent news (Chesney & Citron, 2019). Sowing distrust in institutions, misleading voters, inciting political polarization over caste, religion, and class, can now be done at a never-seen-before scale via fabricated videos and audio recording. This chapter delves into the growing presence of deepfakes in Indian elections, examining their emergence in **2019**, their escalation in **2024**, and the response from regulators, media watchdogs, and fact-checking organizations.

## 4.1: 2019 Elections: The Introduction of Political Deepfakes

While misinformation existed in the previous elections, 2019 elections saw a major wave of deepfake deployment in Indian politics, with AI-generated fake videos, though still nascent in standards, proved to be effective in manipulating voter sentiment.

Intriguingly, legitimate use of deepfake technology was one of the first instances that was widely discussed during the Delhi Assembly Elections in 2020. The BJP released an AI-modified video of a speech by Manoj Tiwari, which saw him speaking in fluent Haryanvi, a dialect he is unfamiliar with. Deepfake technology was used to generate a Haryanvi version of his Hindi speech, to directly appeal to the Haryanvi voter segment in a precision-targeting manner (Sengupta, 2020).

While this deepfake was ultimately benign—it did not spread false information, only adapted existing campaign messaging—it raised ethical concerns about how easily AI could be used to fabricate statements entirely. Experts warned that while Tiwari's deepfake was controlled and intentional, similar technology could be used to create more insidious content, such as fabricated endorsements, false confessions, or manipulated criticisms of political opponents (Banerjee, 2020).

Beyond official campaigns, 2019 also saw the first wave of AI-driven disinformation networks spreading deepfake-generated political content. Fact-checking organizations such as Alt News and BoomLive flagged multiple instances of videos in which opposition leaders appeared to make controversial statements that they had never actually said (Rao, 2021). At the time, deepfake detection tools were limited, and by the time misinformation was debunked, the damage had often already been done.

### 4.3: 2024 Elections: Deepfakes as a Political Weapon

By the time the 2024 general elections arrived, deepfake technology had become significantly more advanced and widely accessible. The shift from experimental AI-generated videos to highly sophisticated deepfake misinformation campaigns was unmistakable. Unlike in 2019, where deepfake use was mostly experimental and localized, 2024 witnessed full-scale disinformation operations, with fabricated videos, AI-generated news anchors, and targeted WhatsApp campaigns influencing millions of voters.

One of the most consequential deepfake incidents of the election involved Rahul Gandhi, a prominent opposition leader. In March 2024, a video surfaced on WhatsApp and Telegram, appearing to show Gandhi praising Pakistan's foreign policy and criticizing India's military decisions. Within hours, the video had been shared across thousands of social media pages and political forums, creating outrage among voters and drawing immediate reactions

from opposition leaders. However, fact-checkers from BoomLive and Factly quickly exposed the video as a deepfake, revealing that AI had been used to alter Gandhi's original speech on international relations (Patel, 2024).

Despite the rapid debunking, the video had already served its intended purpose. Millions of Indians had already seen and formed opinions based on the fabricated clip. This highlighted the speed at which deepfake misinformation could spread and the challenge of fact-checking in real-time. The damage control process required by political figures targeted by deepfakes was often slow and ineffective, as misinformation tends to linger in the public consciousness long after the truth has been revealed (Sharma, 2024).

Another alarming development in the 2024 elections was the use of AI-generated news anchors to spread political propaganda. These synthetic media figures—completely artificial yet hyper-realistic—were deployed by pro-party social media networks to deliver fabricated news bulletins. Unlike traditional misinformation, which relies on altering real clips, these deepfake news anchors were designed from scratch using AI, making them difficult to detect. Their professional appearance and authoritative delivery gave false stories a veneer of credibility that made them even more convincing to the average voter (Bose, 2024).

Meanwhile, deepfake manipulation expanded into regional languages and dialects, making it more challenging for national fact-checking networks to identify and flag content before it went viral. AI-powered WhatsApp disinformation campaigns became more targeted than ever, using deepfake audio messages to impersonate political leaders and influence communities at the grassroots level (Deshmukh, 2024).

### 4.4: The Impact of Deepfake Misinformation on Elections

The unchecked rise of deepfake misinformation has introduced an era of extreme skepticism among voters, where seeing is no longer believing. Public trust in media has deteriorated, with many struggling to discern authentic content from manipulated propaganda (West, 2021). This erosion of truth has had profound implications for democracy, leading to voter confusion, political polarization, and the manipulation of electoral discourse (Hwang, 2020).

Electoral integrity is now under constant threat, as deepfake disinformation campaigns operate at a speed that outpaces real-time fact-checking. By the time fabricated content is identified and debunked, its impact has already shaped public perception. The weaponization of AI-driven misinformation is no longer a hypothetical threat—it is an active force shaping India's electoral future (Maras & Alexandrou, 2019).

### 4.5: The Urgent Need for Deepfake Regulation

As deepfake misinformation continues to evolve, combating it requires a multi-pronged approach. The Election Commission of India (ECI) has already begun enforcing digital campaign regulations, requiring political parties to disclose AI-modified campaign content (Ghosh, 2024). Social media platforms, including Meta and Google, are investing in AI-powered detection tools to filter and flag manipulated media (Choudhury, 2023).

However, the battle is far from over. The 2029 elections may witness an even more advanced era of AI-driven misinformation, potentially making today's challenges seem primitive in retrospect. The only path forward is to strengthen legislation, detection technology, and voter education, ensuring that democracy is protected from the deceptive power of AI.

If left unchecked, deepfakes threaten to make truth irrelevant in political discourse. The future of electoral integrity will depend on how effectively societies can adapt to the deepfake age and fortify their defenses against synthetic media manipulation

## Chapter 5: Electoral System Resilience in India

While India is celebrated as the world's largest democracy, its electoral system carries inherent structural vulnerabilities that often go unnoticed amid the visible vibrancy of mass participation. India's colonially inherited First-Past-The Post electoral system is vulnerable to gerrymandering, disproportional representation, gerrymandering, and vote-bank polarization, despite its simplicity and efficiency (Sridharan, 2012).

In a digital democracy, perceptions, boundaries, and turnouts can be manipulated online and the resilience of the electoral framework is critical to ensure fair outcomes. This chapter explores the limitations of FPTP, looking at the systemic strain points and challenges posed by emerging information warfare tactics in psephological analysis.

### 5.1: The FPTP System and Its Democratic Trade-Offs

In the straightforward FPTP model, the candidate with the most votes wins, irrespective of them securing a majority. This is conducive to a quick, clear outcome, but it can potentially lead to majority governments formed by minority vote shares, raising concerns on the depth of representation in the world's largest democracy that India is.

For instance, in the 2019 Lok Sabha elections the BJP formed the government securing 55% seats with only 37.4% of the vote share and this is not unique to either BJP or Congress or the others, it is a feature of the system. Vote fragmentation enables parties to split opposition votes across multiple candidates, to allow a winner with a lower public mandate, and this has been historically observed across several regional and national elections.

With OSINT coming into play, this raises questions as political entities can take advantage of polarized environments, micro-directing populism towards loyal voter segments over broader consensus-building.

### 5.2: Gerrymandering and the Power of Electoral Geography

Another systemic fragility lies in how electoral constituencies are drawn. Although the Delimitation Commission of India is designed to function independently, accusations of political gerrymandering—the deliberate manipulation of constituency boundaries for electoral gain—have persisted (Palshikar, 2013).

In some Indian states, constituency maps reflect not just population density, but caste and religious fault lines. This leads to the creation of "safe zones" for certain political parties and undermines the principle of equal voter influence. In closely contested states like Uttar Pradesh and West Bengal, the way a constituency is shaped can alter electoral outcomes more than any policy or campaign.

Such engineered geography plays directly into vote-bank politics, where parties mobilize caste or religious blocs for electoral gain. The consequence is a system that incentivizes identity-based polarization rather than democratic deliberation—thereby weakening the resilience of the electoral system to withstand external manipulation and internal fracturing (Yadav, 2016).

### 5.3: OSINT, Disinformation, and Electoral Integrity

In the digital age, the fragility of electoral systems is not confined to ballot processes or constituency maps—it extends into the information ecosystems that shape voter behavior. The Indian electoral environment has increasingly become a battleground of OSINT-driven

disinformation, where adversarial actors exploit systemic weaknesses for strategic gain (Chaudhuri & Kumar, 2023).

The use of AI-enhanced targeting tools, bot-based narrative amplification, and false polling data can distort the electoral field even before a single vote is cast.

OSINT (Open Source Intelligence) tools are now being used by civil society and foreign observers to track election manipulation, identify digital vote-buying attempts, and monitor cross-platform narrative coordination. However, without institutional integration and legal enforcement mechanisms, the insights from OSINT remain reactionary rather than preventive.

**5.4: Countermeasures and Reform Pathways**

To reinforce the resilience of India's electoral system, several structural and technological reforms are being debated. One key proposal is the introduction of proportional representation (PR) in select constituencies or the Rajya Sabha, to correct representational distortions caused by FPTP. While full-scale PR adoption may not suit India's scale and diversity, hybrid systems could offer a balanced alternative.

Another area gaining momentum is delimitation transparency. Activists have called for open-access delimitation data, allowing journalists, civil society, and academic institutions to audit constituency changes and flag gerrymandering attempts in real time. Combined with OSINT-integrated electoral monitoring, such measures could create early warning systems for manipulation.

Finally, there is a growing recognition that electoral system resilience must include digital architecture. The Election Commission of India is now exploring partnerships with AI

researchers and civic tech organizations to create resilient voting infrastructure, deploy deepfake detection, and counter narrative warfare (Basu, 2024).

### 5.5: Rethinking Resilience in Indian Democracy

Electoral resilience is not just about smooth polling days or counting procedures—it's about creating systems that can withstand manipulation, resist polarization, and ensure representative legitimacy. India's electoral system, while robust on paper, reveals deep cracks under the pressure of FPTP distortions, geographic engineering, and digital disinformation.

As the country moves toward the next general elections, the challenge is to build a system that is not only efficient but also ethically durable and technologically fortified. True electoral resilience will require a new blend of legal reform, civic engagement, and digital vigilance—because the integrity of democracy depends not just on casting votes, but on counting them in a fair, representative, and transparent system.

---

## Chapter 6: Influencer-Based Political Advertising in Indian Elections

In the age of digital political warfare, where the battle for attention is fought in feeds and stories, a new kind of political player has emerged—the influencer. Once limited to promoting brands, fashion, or food, social media influencers are now key conduits of political messaging, often more impactful than party spokespeople or traditional media. Influencers have a close connection with niche audiences and a curated target segment, and influencers are increasingly being utilized to influence narratives and mobilize voters, without outrightly declaring affiliations.

India is fertile ground for this, as it is home to over 400 million active social media users. Political parties now engage micro- and macro-influencers to disseminate campaign messages, subtly shape public opinion, and flood social media with coordinated yet organic-seeming content (Kaur & Narayan, 2021). This chapter explores how influencer-based advertising is transforming electioneering in India—unregulated, powerful, and often invisible to the average voter.

### 6.1: The Blurring Line Between Influence and Propaganda

Unlike traditional political advertisements, which are marked and regulated, influencer content often flies under the radar of election commission scrutiny. A tweet, meme, or Instagram reel supporting a candidate may not be classified as an advertisement—yet it functions as one, especially when posted in a coordinated fashion across hundreds of accounts.

During the 2019 general elections, the BJP's digital strategy included influencer outreach programs targeting YouTubers, meme pages, and Instagram creators. Some

influencers were invited to party events and given exclusive access in exchange for coverage. A similar strategy was visible in the 2022 Uttar Pradesh assembly elections, where regional influencers posted “unpaid” endorsements of political parties while receiving monetary incentives or free promotions from PR agencies linked to campaigns (Tripathi, 2023).

The issue isn’t just sponsorship—it’s opacity. Most influencer posts contain no disclosure labels, making it difficult for users to distinguish genuine opinion from paid promotion. This manipulation of trust is a hallmark of influencer-based political advertising and poses a significant challenge to transparency in democratic discourse.

### 6.2: Regulatory Grey Zones and the Role of the Election Commission

While India’s Representation of the People Act (1951) and Election Commission of India (ECI) guidelines cover political advertisements on traditional and digital media, influencer content exists in a regulatory vacuum. Platforms like Instagram, Twitter (X), and YouTube are not legally obligated to flag influencer content as paid political speech unless explicitly sponsored.

In 2022, the ECI issued a notice to political parties warning against “covert social media promotion” by influencers but has yet to implement a clear enforcement mechanism or disclosure rulebook (ECI Notice, 2022). Meanwhile, the Advertising Standards Council of India has guidelines for influencer marketing but lacks jurisdiction over political speech (ASCI, 2021).

There creates a gap as essentially, political advertising is unregulated and algorithmically enabled, and this can make it difficult for voters to critically examine the source of political content, thereby undermining electoral transparency.

### 6.3: Implications for Democracy and OSINT Monitoring

Influencers are essentially content creators who can sway public opinion and this adds in a layer of asymmetry, as political actors with resources to utilize influencers can have higher reach. If they subtly talk about a political party, without naming the party even, there is no scope for accountability.

For OSINT analysts and electoral monitors, this raises two critical challenges:

1. Detection Complexity: There is no set format for influencer posts and its primary nature as entertainment content makes it hard for algorithms to detect that it is, in fact, coordinated political messaging.
2. Attribution Ambiguity: Without formal linkages to campaigns or any financial disclosures, it isn't easy to trace influencers' affiliations to their political sponsors.

Network-based analysis, methods to identify patterns of hashtag coordination, patterns of simultaneous posting and echo chambers, are some of the aspects that need to be included in OSINT frameworks to solve this problem. Influencer mapping by using AI-powered metadata analysis can potentially aid in this.

### 6.4: From Soft Power to Sharp Power

Influencers are essentially soft-power agents in the algorithmic ecosystems and in the context of elections, it becomes a sharp power, shaping voter preferences in ways bypassing scrutiny.

As India prepares for future elections, transparency in influencer-based political content must become a regulatory and civic priority. Electoral integrity depends not only on counting ballots but also on tracing influence, especially in the digital spaces where millions

now cast their psychological votes long before polling day.

# Chapter 7: Algorithmic Influence and the Role of AI in Indian Elections

In today's India, algorithms are also political actors, as they decide what voters see, hear, believe, and perceive. The hundreds of millions of Indians that use Facebook, YouTube, and Instagram, are impacted by opaque curation, personalization, and amplification algorithms, and these algorithms are unaccountable when it comes to political discourse.

## 7.1: Filter Bubbles and Echo Chambers

Algorithmic social media tends to create filter bubbles where users see only the content that reinforces their beliefs and this eventually leads to the users experiencing echo chambers where their opposite views are muted, resulting in a deepened polarization.

Farm laws, Citizenship Amendment Act (CAA), Article 370, are some of the instances where algorithm-led personalization caused ideological ghettoization (Pandey & Parashar, 2024), with users getting nudged towards echo chambers reinforcing their political beliefs. These bubbles reduce voter exposure to diverse perspectives, weakening deliberative democracy.

## 7.2: AI-Amplified Disinformation

AI tools can now predict what can go viral, considering the wealth of data that exists openly on social media. Researchers have observed that the 2019 and 2024 elections saw polarizing content receive more algorithmic amplification than policy-focused information (Ünver, 2023).

Algorithms are trained on engagement metrics - likes, comments, watch time - and not on accuracy or democratic impact or political affiliation, and this makes it difficult for platforms to intervene.

### 7.3: Emerging Threat: AI-Generated Political Propaganda

With the rise of generative AI tools like ChatGPT and Midjourney, Indian political campaigns are outsourcing propaganda creation to machines, as observed in the use of AI-generated images, memes, and tweets supporting various political actors in the recent elections.

What makes this dangerous is that AI content is hard to trace, easy to scale, and visually persuasive. Platforms lack both the will and the tools to track such content unless it violates explicit community standards. The result? Synthetic populism—manufactured at scale, optimized for outrage, and impossible to counter in real time.

### 7.4: Policy Gaps and Democratic Risk

Despite their enormous influence, platforms operating in India are not required to disclose how their algorithms function during elections. There is no mandated transparency on:

- How content is prioritized
- How political ads are targeted
- Whether specific ideologies are being algorithmically boosted

This opacity makes it impossible for civil society or regulators to assess electoral bias or manipulation. Algorithms that shape public opinion during an election remain black boxes, even to the Election Commission.

### 7.5: Toward Algorithmic Accountability

Algorithms may be technical, but their impact is profoundly political. As India heads into a hyper-digital electoral future, it is imperative that AI systems are made subject to democratic oversight.

We need public policy frameworks that ensure:

- Transparency in recommendation systems during elections
- Equal moderation standards across languages and regions
- Disclosure of AI-generated political content
- Third-party audits of political content amplification

OSINT systems must now evolve to monitor not just what users post—but what algorithms prioritize.

---

# Chapter 8: Cross-Platform Coordination in Indian Elections

In the current digital era, political campaigns in India are no longer confined to speeches, press releases, or platform-specific outreach. They unfold through tightly synchronized networks that span multiple digital ecosystems—from private WhatsApp forwards and Telegram channels to viral Instagram memes, YouTube explainers, and coordinated tweet storms.

Cross-platform coordination is a significant evolution in political communication, as modern campaigns can now design narrative clusters across platforms. A tweet can become a meme, video, or even a headline based on how it is utilized in other platforms, shaping public opinion in real time. In the Indian context, cross-platform coordination is both a strategic asset for political parties and a major structural challenge for democratic transparency.

## 8.1: Narrative Engineering: Multi-Platform Message Design

Cross-platform campaigning doesn't happen accidentally—it's a **deliberate architecture**. Political campaigns are often designed with a multi-platform perspective (Pandey & Parashar, 2023). A campaign video may first premier on YouTube, and clips of that can be shared as reels on Instagram or forwarded on WhatsApp, or framed as a poll on Twitter; options and means are basically endless.

This allows political narratives to:

- Reach **diverse demographics** (youth on Instagram, elders on WhatsApp)
- Maximize **repetition across formats**, reinforcing recall
- Escape detection or censorship by **mutating contextually**

### 8.2: Campaigns in Disguise

As discussed earlier in the paper, coordinated inauthentic behaviour, via fake accounts and bots across platforms can create trends of false support or outrage, and can dominate platforms.

In 2022, Meta took down an India-based network of over 700 accounts linked to a digital marketing firm promoting a party across Facebook, Instagram, and WhatsApp. Same messaging was shared in modified formats in these accounts, with the timing of the posts coinciding with major speeches, elections, or any other politically significant events (Meta Transparency Report, 2022).

Reposting links from one platform to another, ensuring hashtags are communicated directly on WhatsApp groups, and operating in various languages is a key aspect of cross-platform campaigning. This lets campaigns bypass existing media filters.

Another key element is the recontextualizing of information, as the same information can be told in a different context and in a different tonality, like a meme or a voice note or a report. This ‘memefication’ across different platforms can allow the same information or misinformation to take multiple forms; bypassing detection systems while reinforcing echo chambers across platforms.

### 8.3: OSINT and Election Oversight: Why Single-Platform Monitoring Fails

For election monitors and OSINT frameworks, cross-platform coordination poses major barriers:

- Fragmented Content: The same message appears differently on every platform, breaking keyword detection systems.
- Encrypted Messaging: WhatsApp and Telegram offer limited visibility.

- Lack of Real-Time Tracking: Coordination is often detected after the impact is felt.

Tracking elections now requires inter-platform analysis—mapping how one message triggers cascades across systems.

### 8.4: Coordinated Regulation for Coordinated Campaigns

India's electoral future is not just digital—it's interconnected across invisible infrastructures. To protect democratic integrity, election oversight must match the coordination of digital campaigns. This means:

- Mandating platforms to share political content data in real-time
- Establishing a cross-platform Election Disinformation Task Force
- Allowing third-party researchers API access for election cycles
- Building AI tools to detect narrative coordination, not just content violations

Ultimately, cross-platform coordination can't be stopped—but it can be monitored, made transparent, and held to democratic standards.

---

# Chapter 9: Practitioner Perspectives on OSINT in Indian Electoral Campaigning

## Qualitative Data Analysis Methodology

Participants with expertise in political consulting, social media strategies, and other OSINT applications were selected and consented audio-recorded interviews were conducted. These interviews were transcribed verbatim, with each interview being 30-45 minutes.

### 9.1: Thematic Analysis

Braun and Clarke's six-step framework was used to identify themes systematically:

1: Familiarisation

All the transcripts were reviewed thoroughly to ensure familiarisation with the topic.

2: Initial Coding

Initial coding was done to highlight significant concepts, statements, and practices. Examples include:

- "Microtargeting by booth-level"
- "Ethically uncomfortable"
- "Facebook benefits from propaganda"
- "No consent for data use"
- "Strategic WhatsApp forwards"

3: Focused Coding

Initial codes were grouped based on conceptual similarity into broader categories (axial codes). For instance:

- "Microtargeting" and "live sentiment monitoring" → Campaign Operational Techniques
- "Memes as political tools" and "satirical manipulation" → Narrative Engineering
- "No consent" and "data misuse" → Voter Privacy and Ethical Discomfort

4: Developing Themes

The themes were further developed to capture recurring patterns that were significant to research questions:

- OSINT as a Campaign Imperative: Central role of OSINT in real-time electoral strategies.
- Strategic Use and Misuse: OSINT's dual-use nature in persuasion and manipulation.
- Ethical Tensions and Voter Privacy: Ethical concerns regarding consent and privacy in OSINT usage.
- Role of Technology Platforms: Influence and shortcomings of digital platforms like Facebook and WhatsApp.
- Policy Gaps and Suggestions: Expert recommendations on necessary regulatory and policy interventions.

5: Defining and Naming

Each theme was defined clearly to ensure they accurately represent the data, with depth and clarity being ensured by illustrative quotations like:

- Ethical concerns: "It's an open secret that we scrape social media... but no one tells the user their data is being used."

- Regulatory gaps: "The Election Commission is not equipped to audit memes or WhatsApp forwards in real time."

6: Producing The Report

All of the thematic insights were structured cohesively, to present the practitioner perspectives as below.

**9.2: A Qualitative Analysis of Expert Interviews**

To deepen the understanding of how Open Source Intelligence (OSINT) operates within the lived realities of Indian elections, five semi-structured interviews were conducted with professionals in political strategy, digital communications, and technology. The insights were anonymized using pseudonyms and analyzed thematically to uncover key patterns, ethical tensions, and regulatory gaps. These interviews ground the theoretical and case-based discussions from earlier chapters in the empirical realities of campaign operations.

**9.3: Thematic Analysis**

1. OSINT as a Campaign Imperative

Across all interviews, it was clear that OSINT has transitioned from a niche skill to a mainstream campaign requirement. Whether through social media scraping, trend tracking, or cross-referencing public databases, OSINT enables granular voter targeting and rapid message adaptation.

- *Ravi* (Political Consultant) noted how campaign teams monitor live sentiment shifts on Twitter and adjust message tone within hours.
- *Aarav* (Digital Strategist) emphasized the merging of electoral rolls, demographic data, and past voting behavior to prioritize booth-level campaign resources.

2. Strategic Use and Misuse

While OSINT offers tactical advantages, interviewees also described its dual-use nature. Several admitted to having observed or been part of campaigns where OSINT was used to create misleading or emotionally manipulative narratives.

- *Kabir* (Communications Lead) described meme and satire strategies used to "troll without direct trolling," influencing low-literacy voter segments through indirect ridicule.
- *Dev* (Campaign Analyst) illustrated a long-term narrative construction strategy via influencer networks to shape perceptions about a future Prime Ministerial candidate.

3. Ethical Tensions and Voter Privacy

Every participant flagged ethical discomfort with how OSINT is applied in political contexts—especially when public data is used without informed consent.

- *Ravi* questioned the morality of inferring voter behavior from social media without the user's awareness.
- *Ishaan* (Tech Project Manager) pointed to the "open secret" nature of OSINT, where data is public but not meaningfully transparent, leading to asymmetric power between campaigners and citizens.

4. The Role of Technology Platforms

Most participants expressed concern over the unregulated influence of platforms like Facebook, WhatsApp, and Instagram. These services often profit from political traffic but fail to disclose algorithmic behavior or enforce consistent moderation.

- *Kabir* discussed the lucrative nature of propaganda for tech companies and the lack of third-party oversight.
- *Ishaan* emphasized that even where platform policies exist, enforcement is minimal in regional languages.

5. Policy Gaps and Suggestions

A common theme across interviews was the urgent need for proactive digital election regulation. Suggestions included:

- Mandatory disclosures for AI-generated content in campaigns.
- Platform transparency in algorithmic curation of political material.
- Privacy-first legislation for the use of voter-related OSINT.

Interviewees emphasized that India's democratic infrastructure is **playing catch-up** with the pace of political technology.

---

# Chapter 10: Regulatory and Policy Gaps in India's Digital Electoral Ecosystem

India has one of the most exhaustive, logistically advanced election infrastructure in the world, with a well-defined legal structure. However, there are still gaps in the context of the rapidly evolving landscape of digital campaigning.

While the Election Commission of India has strong procedural control over conventional campaigns, there are still regulatory gaps when it comes to AI, social media platforms and encrypted messaging apps. This results in an ecosystem where political actors benefit from disinformation, micro-targeting, and misinformation.

There is a need to examine the legal, institutional, and operational gaps in India's response to the digital disruption in the Indian electoral system.

## 10.1: Gaps:

### *10.1.1: Legal and Institutional Silos*

The Representation of People Act (1951), written in the age of newspapers and loudspeakers, does not have literature on:

- Political messaging on WhatsApp or Telegram
- Targeted social media advertisements
- Disinformation disguised as satire or influencer content

ECI does not have explicit jurisdiction over digital campaigns and other means of cooperation from platforms is needed to regulate (Lohani, 2021).

### *10.1.2: The Limits of Platform Self-Regulation*

India's current regulatory ecosystem relies on self-regulation by platforms, with social media companies being expected to voluntarily curb misinformation and political manipulation. But studies show this model is fundamentally flawed:

- Platforms apply inconsistent moderation in regional languages
- Enforcement is often reactive, not preventive
- Political content is amplified based on engagement, not accuracy

Ashwini (2021) highlights that under the Intermediary Guidelines & Digital Media Ethics Code Rules (2021), platforms are only required to act after complaints—not proactively detect coordinated campaigns.

### *10.1.3: Electoral Silence and the Digital Loophole*

The ECI mandates a 48-hour "electoral silence period" before voting, restricting campaigns and media commentary. But this rule is routinely violated online.

In the 2022 Uttar Pradesh elections, Twitter and Telegram saw a surge of "forwarded polls," meme campaigns, and attack ads during this blackout window. Platforms claimed ignorance; the ECI lacked the enforcement tools to act.

Schwertheim et al. (2024) note that digital blackouts are nearly impossible without real-time API access, algorithmic accountability, and pre-scheduled moderation agreements.

### *10.1.4.: No Rules for Political Microtargeting*

Unlike the EU or USA, India has no mandatory disclosure of political ads on digital platforms, and no audit system for targeting algorithms.

This creates a dangerous space where:

- Political actors can microtarget users based on religion, caste, or language
- Voters may receive entirely different campaign messages, unseen by regulators
- There is no public record of who paid for which messages

As Shankar & Ahmad (2021) explain, this lack of transparency turns social media into a "shadow public sphere", invisible to both regulators and citizens.

### *10.1.5: Missing Electoral Cybersecurity Protocols*

India's regulatory structure is also blind to bot networks, coordinated inauthentic behavior (CIB), and AI-generated content. During the 2023 Karnataka elections, several AI-generated memes were traced to external servers, but no legal provision existed to classify or penalize them. While cybercrime laws exist, they don't map well to electoral interference—which is structural, not individual.

### *10.1.6: Regulatory Capture and Political Incentives*

Finally, there's the problem of regulatory capture. Many digital platforms have been accused of favouring ruling parties in content moderation and ad policies. The ECI has no independent audit mechanism to verify neutrality or detect suppression.

UNDP (2023) recommends third-party election integrity audits, modeled on Brazil's and Germany's digital oversight boards, which operate with public participation and platform liability.

## 10.2: Building a Future-Proof Electoral Framework

India's elections are entering a new phase—digitally sophisticated, AI-influenced, and platform-mediated. But the institutions protecting these elections remain analog.

To close the regulatory gap, India must pursue:

- Comprehensive digital election law reform
- Pre-emptive coordination protocols with platforms during election seasons
- Mandated political ad transparency and microtargeting disclosures
- Independent oversight bodies empowered to issue binding directions
- Real-time OSINT integration for fact-checking, content tracing, and public alerts

Regulation must balance freedom of expression with systemic integrity—protecting not just free speech, but the conditions that make it meaningful.

India does not lack electoral expertise—it lacks digital vigilance. The moment to build it is now.

---

## Chapter 11: Conclusion and Future Scope

OSINT has transformed the way elections are conducted, analysed, and influenced and this study examined the radical transformation that OSINT has brought in in Indian electoral politics in 2014, 2019, and 2024 general elections. Via secondary data analysis and qualitative expert interviews, this research has brought to light how OSINT tools like social media analytics, AI-based targeting, deepfake technologies, and more have shaped the modern political communication and campaign strategies.

One of the key findings is that OSINT is dual natured - it enables efficient, real-time data-driven campaigning that aids in enhancing democratic engagement and inclusivity and on the other hand, it brings threats like misinformation, algorithmic manipulation, micro-targeting in a non-consensual manner, and deepfake propaganda among others. These can undermine democratic intergrity and distort electoral outcomes.

Chapters 2-8 dive deep into the mechanics of this transformation, from how campaigns started being hybrid, blending online and offline methodologies; to algorithmic recommendations systems aiding political actors in utilising open platforms for both overt and covert electoral gains. Chapter 9 established these findings in the lived experiences of practitioners, who revealed the dual nature - strategic advantage and ethical concerns - brought in by OSINT; apart from shedding light on the regulatory gaps prevalent in the system.

The research also has found that India’s regulatory architecture has not been able to keep up pace with the rapid digitalisation of electoral campaigning, as existing frameworks are ill-equipped to handle emerging campaign strategies like AI-generated misinformation,

covert influencer marketing or real-time micro targeting. Which is why the concluding chapters, 9 and 10, talk about the need for algorithmic accountability, proactive regulation, platform transparency, and digital literacy to ensure democratic integrity is sustained in the digital age.

OSINT democratizes information access and political participation but it also puts power in the hands of those with the resources to weaponise data and information. OSINT is a paradox that has emerged in the electoral contexts and is here to stay.

### 11.1: The Way Forward

The way forward is to ensure there is a comprehensive study, analysis, and policy development.

There is a necessity to have large-scale surveys to understand the impact of OSINT-driven political content on voter behaviour, apart from its impact on trust in elections. This has to be done over multiple election cycles at various levels. This would also include the development of AI-powered OSINT monitoring tools for real-time monitoring of any of the methods listed in this study.

This research will also bring out the impact of various regulatory approaches, including algorithmic-accountability and platform transparency, in countering electoral manipulation online. Furthermore, there is a need to understand how OSINT-led campaigns function in India’s vastly multilingual landscape, as localised influencers and vernacular content plays a critical role in voter behaviour.

The policy research in this context can also lead to interventions focusing on digital literacy to equip citizens with the skills needed to identify deepfakes, fact-check with OSINT by themselves, and evaluate digital content.

### 11.2: Final Thought

OSINT in electoral contexts is not just a technological issue, it is a democratic issue and there is a need for academically rigorous, ethically-robust research to ensure democratic integrity is maintained and sustained.

## Bibliography

**Aneez, Z., Neyazi, T. A., Kalogeropoulos, A., & Nielsen, R. K. (2019).** *Online disinformation in the run-up to the Indian 2019 election*. Reuters Institute for the Study of Journalism.

**Bradshaw, S., & Howard, P. N. (2018).** *The global organization of social media disinformation campaigns. Journal of International Affairs, 71*(1.5), 23-32.

**Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016).** *The rise of social bots. Communications of the ACM, 59*(7), 96-104.

**Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2020).** *The IRA, social media and political polarization in the United States, 2012-2018*. Computational Propaganda Research Project.

**Jakesch, M., Garimella, K., Eckles, D., & Naaman, M. (2021).** *Trend alert: How a cross-platform organization manipulated Twitter trends in the Indian general election*. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW1), 1-18.

**Bradshaw, S., & Howard, P. N. (2018).** *The global organization of social media disinformation campaigns. Journal of International Affairs, 71*(1.5), 23-32. https://www.jstor.org/stable/26508115

**Christopher, N. (2024).** *Indian Voters Are Being Bombarded With Millions of Deepfakes. Political Candidates Approve.* Time Magazine.

**Ghosh, A. (2024).** *AI and Deepfakes Blur Reality in India Elections.* BBC News.

**Jakesch, M., Garimella, K., Eckles, D., & Naaman, M. (2021).** *Trend alert: How a cross-platform organization manipulated Twitter trends in the Indian general election*. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW1), 1-18.

**Lakshané, R. (2024).** *Political AI: The Role of AI and Deepfakes in India's Elections.* The Wire.

Chadwick, A. (2017). *The Hybrid Media System: Politics and Power.* Oxford University Press.

Chakravartty, P., & Roy, S. (2015). *Mediatized Populisms: Narendra Modi and the 2014 Indian Elections. Journalism*, **18**(2), 195-213.

Pal, J., Chandra, P., & Vydiswaran, V. (2016). *Social Media and Political Engagement in India's 2014 Elections. The International Journal of Press/Politics*, **21**(3), 398-416.

Rao, S. (2020). *Digital Politics in India: Social Media and Political Campaigning. Journalism Studies*, **21**(10), 1360-1378.

Singh, A. (2024). *Artificial Intelligence and Electoral Campaigning in India. arXiv preprint.*

Ahmed, R. (2015). *Social Media and the Political Participation of Indian Youth: An Empirical Study. Asian Journal of Communication*, **25**(1), 86-101.

Mahapatra, S. (2015). *Role of Social Media in Indian Politics: A Case Study of 2014 Elections. International Journal of Humanities and Social Science Invention*, **4**(2), 12-19.

Jaffrelot, C. (2015). *The Modi-centric BJP 2014 Election Campaign: New Techniques and Old Tactics. South Asia: Journal of South Asian Studies*, **38**(4), 719-735.

Chaturvedi, S. (2019). *How India's Political Parties Are Using Data Analytics and AI to Win Elections. Economic and Political Weekly*, **54**(5), 48-57.

Aneez, Z., Neyazi, T.A., & Ranganathan, M. (2020). *The WhatsApp Election: Political Messaging and Mobilization in India's 2019 General Elections. Asian Journal of Communication*, **30**(1), 22-38.

Tripathi, R. (2020). *Pop Culture and Political Campaigns in India: The Case of #PoonamPhirSe. Journal of Media and Cultural Studies*, **34**(2), 76-92.

Sengupta, A. (2023). *AI-Driven Election Campaigns: The Future of Political Strategy in India. Indian Journal of Political Science*, **84**(1), 56-75.

Ganguly, P. (2023). *Data Analytics and AI in Indian Elections: A New Age Hybrid Campaigning Strategy. South Asian Journal of Political Studies*, **12**(3), 123-145.

Sharma, K. (2024). *Geo-fencing and Digital Mobilization in Indian Elections. Journal of Political Technology*, **6**(2), 90-110.

Chaudhuri, A. (2023). *Deepfakes, AI, and Election Integrity in India. Media and Communication Journal*, **58**(4), 112-134.

**Chesney, R., & Citron, D. (2019).** *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Politics.* Foreign Affairs.

**Narayanan, A., Kapoor, P., & Chawla, K. (2020).** *Misinformation and Deepfakes in Indian Elections: A Case Study.* Journal of Digital Ethics.

**Paris, B., & Donovan, J. (2019).** *Deepfakes and Synthetic Media: The Perversion of Truth in the Digital Age.* Data & Society Research Institute.

**Sengupta, A. (2020).** *The Use of Deepfakes in Indian Elections: A New Challenge for Political Campaigns.* South Asian Journal of Political Studies.

**Kumar, S. (2020).** *Deepfake Technologies and Political Disinformation in India's 2019 Elections.* International Journal of Digital Communication.

**Banerjee, P. (2020).** *The Ethical Implications of AI-Generated Political Content: Case Study of BJP's Deepfake Campaign.* Indian Journal of Political Science.

**Gupta, R. (2021).** *Weaponizing Deepfake Technology: Disinformation and Electoral Manipulation in India.* Asian Journal of Communication.

**Rao, S. (2021).** *The Role of Fact-Checkers in Combating Deepfake Misinformation in Indian Elections.* Media and Communication Journal.

**Patel, V. (2024).** *Deepfake Video Manipulation in the 2024 Elections: Rahul Gandhi Case Study.* Indian Political Review.

**Sharma, K. (2024).** *Fact-Checking in the Age of AI: Strategies to Counter Deepfake Misinformation in Elections.* Journal of Digital Forensics.

**Bose, M. (2024).** *The Rise of AI-Generated News Anchors in Indian Elections: A New Disinformation Strategy.* South Asian Media Studies Journal.

**Deshmukh, A. (2024).** *The Spread of Deepfake Misinformation via WhatsApp: Examining Regional Language Targeting.* Journal of Misinformation Studies.

**West, D. M. (2021).** *Deepfakes and Democracy: The Impact of AI-Generated Disinformation on Voter Trust.* Brookings Institution Report.

**Hwang, T. (2020).** *Deepfakes, Synthetic Media, and the Fight Against Digital Manipulation.* Ethics and AI Journal.

**Maras, M., & Alexandrou, A. (2019).** *Determining the Threat of Deepfake Misinformation in Global Elections.* Journal of Cybersecurity Studies.

**Ghosh, P. (2024).** *Regulating Deepfake Technology: The Election Commission of India's New Digital Campaign Policies.* Indian Law Review.

**Choudhury, R. (2023).** *How AI Detection Tools are Combatting Deepfake Misinformation on Social Media.* Journal of Emerging Technologies.

**Reddy, S. (2024).** *AI-Assisted Fact-Checking Networks: Combating the Next Wave of Digital Misinformation.* Media Ethics Journal.

**Sridharan, E. (2012).** *Coalition Politics in India: Selected Issues at the Centre and the States.* Institute of South Asian Studies.

**Vaishnav, M. (2017).** *When Crime Pays: Money and Muscle in Indian Politics.* Yale University Press.

**Palshikar, S. (2013).** *Indian Democracy: Meanings and Practices.* SAGE Publications India.

**Yadav, Y. (2016).** *Caste, Community and the Constituency: Transformations in Indian Electoral Politics.* Seminar Magazine, Issue 674.

**Chaudhuri, K., & Kumar, A. (2023).** *Weaponizing Misinformation: OSINT and Electoral Manipulation in India.* Journal of Digital Security.

**Narayanan, V., Das, P., & Iyer, S. (2023).** *Social Media Warfare in Telangana Elections: OSINT Lessons.* Digital Democracy Review.

**Kapoor, A., & Mehta, P. (2022).** *Is It Time for Proportional Representation in India?* The Hindu Centre for Politics and Public Policy.

**Basu, R. (2024).** *AI and Election Monitoring: Building Resilient Electoral Infrastructure in India.* Journal of Civic Tech & Policy.

**Kaur, S., & Narayan, S. (2021).** *The Political Economy of Influencers: How Social Media Personalities Shape Indian Elections.* Journal of Political Communication.

**Tripathi, R. (2023).** *Influencer Elections: The Rise of Politainment in Indian Democracy.* Media & Democracy Review.

**Ravindran, P. (2023).** *Instagram Reels and Political Engagement: A Study of Youth Voting in Karnataka.* Journal of Youth Politics.

**Election Commission of India (2022).** *Guidelines on Political Advertising and Social Media Conduct.*

**Advertising Standards Council of India (ASCI) (2021).** *Guidelines for Influencer Advertising on Digital Media.*

**Sundar, S., & Iyengar, R. (2023).** *Mapping Influence Networks in Indian Elections: A Framework for OSINT-based Detection.* Journal of Digital Intelligence.

**Qureshi, M. (2020).** *Misinformation During the Anti-CAA Protests: A Case Study.* Media and Politics Review.

**Mehrotra, A. (2021).** *Sharjeel Imam Deepfake Case: Disinformation as a Weapon.* Digital Law Journal.

**Chakraborty, A., et al. (2021).** *Lexical Variants and Evasion in Indian Political Misinformation.* Proceedings of the ACL Workshop on Online Abuse and Harms.

**Singh, R., & Roy, T. (2022).** *Evasive Misinformation Tactics in Indian Elections.* Journal of Social Media Studies.

**Desai, P. (2023).** *WhatsApp Misinformation in Karnataka Elections.* Election Media Studies Quarterly.

**Aneez, Z., Neyazi, T., & Sinha, R. (2020).** *Bot Activity in India's 2019 General Elections.* Asian Journal of Communication.

**Kulkarni, M. (2022).** *Gujarat Elections and Communal Misinformation Networks.* South Asia Security Review.

**Narayanan, A., Iyer, S., & Das, V. (2023).** *AI-Generated Misinformation in Telangana Elections.* Open AI Policy Forum.

**Iyer, R., & Basu, T. (2023).** *Fake Polling Data as Election Interference.* Indian Journal of Electoral Studies.

**Jain, P., & Varma, S. (2020).** *Symbolic Language in Political WhatsApp Campaigns.* Technology & Democracy Journal.

**Kapoor, V. (2022).** *The Election Commission and the Limits of Misinformation Oversight.* Public Policy India Review.

**Rajan, S., & Mehta, D. (2022).** *Behavioral Metadata in Election Disinformation Campaigns.* OSINT & Democracy Series.

**Pandey, R., & Parashar, R. (2024).** *Digital Spaces and Political Mobilisation in India: An Algorithmic Perspective.*

**Ünver, H. A. (2023).** *New Methods of Information Manipulation in Elections: The Role of AI and Virality.*

**Kulkarni, A., & Sinha, R. (2023).** *Language Disparities in Algorithmic Moderation: A Case Study of Indian Elections.*

**Raj, S., Menon, T., & Basu, P. (2023).** *AI-Generated Political Messaging in India's Regional Elections.*

**Sharma, V., & Rout, S. (2024).** *Algorithmic Accountability and Electoral Integrity: The Indian Imperative.*

**Tiwari, A., Bhatia, D., & Joshi, M. (2023).** *Monitoring Algorithmic Bias in Political Communication: A Civic OSINT Framework.*

**Pariser, E. (2011).** *The Filter Bubble: What the Internet Is Hiding from You.* Penguin Press.

**Ghosh, M., & Narayanan, A. (2023).** *Platform Inequality: How Regional Language Users Face Algorithmic Disadvantage.*

**Lohani, M. (2021).** *Digital Campaign Finance and Electoral Transparency in India.* Observer Research Foundation Occasional Paper.

**Ashwini, R. (2021).** *Perspectives on Platform Regulation in India.* In: S. Gorwa (ed.) *Platform Governance & the Public Interest.*

**Schwertheim, C., Colliver, C., & Fagan, C. (2024).** *Safeguarding Elections in the Digital Age: Disinformation and Democratic Resilience.* Institute for Strategic Dialogue.

**Shankar, B., & Ahmad, A. (2021).** *Shadow Public Spheres: Microtargeting in Indian Elections.*

**Tan, Y. (2020).** *Election Law, Cybersecurity, and the Challenge of Coordinated Disinformation. Election Law Journal*, 19(4), 345–358.

**United Nations Development Programme (2023).** *Information Integrity to Sustain Peace During Electoral Processes.*

**Marsden, C., Brown, I., & Veale, M. (2021).** *Strengthening Electoral Integrity Through Digital Oversight: A Rights-Based Framework.* University College London.

**ISD Global (2024).** *Election Integrity and Platform Accountability: Real-Time Monitoring and Response Models.*

**Basu, A. (2023).** *The Limits of the Election Commission's Digital Oversight Powers in India. India Forum.*

**Gurumurthy, A., & Bharthur, D. (2022).** *Regulating Big Tech in the Indian Context: Lessons from Electoral Disinformation Cases.* IT for Change.

**Herf, J. (2006)**. *The Jewish Enemy: Nazi Propaganda during World War II and the Holocaust*. Harvard University Press.

**Tickner, L. (1988)**. *The Spectacle of Women: Imagery of the Suffrage Campaign 1907–14.* University of Chicago Press.

**TRAI (2023)**. *Internet and Mobile Data Usage in India: Annual Report*. Telecom Regulatory Authority of India.