*Page 741 - 753* **DOI:** *https://doij.org/10.10000/IJLMH.1110821*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 8 | Issue 5**

**2025**

# From Booth Capturing to Algorithm Manipulation: Emerging Threats to Indian Electoral Sovereignty in the Era of Digital and Remote Voting

VIJAY KUMAR[1]

**ABSTRACT**

*India, the world's largest democracy, has made commendable strides in securing the electoral process against traditional threats like booth capturing and ballot stuffing largely through the successful implementation of Electronic Voting Machines (EVMs). However, as India stands on the cusps of a new era defined by digital governance, social media ubiquity, and the proposed introduction of remote voting , a new generation threats is emerging. This paper examines the evolving threats to India's electoral sovereignty and its integrity, representing a critical transition from traditional , physical vulnerabilities to complex , digitally driven . This research paper argues that while the Election Commission of India (ECI) has effectively fortified the physical ballot, the new challenge for electoral sovereignty is digital threats such as algorithmic manipulation, misinformation compaign on social media , cybersecurity challenges in remote voting infrastructure . This paper analyzes the nature of these emerging threats, examines their potential impact on India,s electoral sovereignty, and proposes a multi-pronged strategy encompassing robust legislative frameworks, technological safeguards and enhanced enhanced institutional capacity to preserve democratic integrity in the 21st century.*

***Keywords****: Elections, Electoral Sovereignty, Digital Voting, Remote Voting, Algorithmic Manipulation, Cybersecurity, Election Commission of India, Booth Capturing, Indian Democracy.*

## I. INTRODUCTION

The sanctity of the vote is the bedrock of any functioning democracy. India's democratic experience is a spectacle of unparalleled scale and complexity. With an over **96.88** crore electors registered across the country (around 8% increase in registered voters from 2019)[2] , conducting a free, fair, and transparent election is a monumental logistical and administrative

[1] Author is a LL.M. Student at Lovely Professional University, India.
[2] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2005189

 [ISSN 2581-5369]

achievement. For decades, the primary narrative surrounding the security of the Indian vote was one of overcoming brute-force tactics. The phrase booth capturing!- the physical occupation of a polling place to cram ballot boxes - used to be the biggest menace to electoral integrity. Such practices were pushed to the history book by the Election Commission of India (ECI) as a result of several radical reforms[3]. The introduction of a gradual use of Electronic Voting Machines (EVMs) that began in 1998[4], the rigorous adherence to the Model Code of Conduct, and the introduction of central security forces, were cleansing the process of polling, which became more transparent and efficient.

But the world was shifting in a seismic change with respect to technology as India solidified its reputation of having solid elections. The spread of the internet, the ubiquity of smartphones, and the emergence of social media applications all have changed the nature of political speech and, therefore, the difficulties in electoral persuasion. These threats are no longer located in the physical realm of a polling booth, but they are now decentralized, digital and are mostly invisible.

In this paper, a critical analysis of this evolutionary path has been described. Its main area of carrying out the analysis is that the threats to the electoral sovereignty of India have grown beyond the physical acts of coercion by algorithm-based manipulations being directed to the epistemological and foundational knowledge of a democratic state. The aim of the booth capturing was to dominate the ballot, whereas the new breed of threats aims at dominating the voter , his perceptions, beliefs and eventually his choice and the way of voting. This transformation is a much more sinister challenge because it is more difficult to spot, more difficult to blame and the results are more vaporous to social integrity and civil relations.This research will proceed in several parts following :-

- It will start, first, by giving a historical background through revisiting the time of the booth capturing and the successful countermeasures of the ECI to form a baseline of the challenges faced in the past.
- Second, it will examine the present situation with social media weaponization to spread disinformation, the susceptibility of electoral data, and election infrastructure cyber-attacks.
- Third, it will examine the new frontier of remote and digital voting, where the level of

[3] Sridharan, E., & Vaishnav, M. (2017). Election Commission of India. In *Oxford University Press eBooks*. https://doi.org/10.1093/oso/9780199474370.003.0011

[4] Wikipedia contributors. (2025, March 15). *Electronic voting in India*. Wikipedia. https://en.wikipedia.org/wiki/Electronic_voting_in_India

 [ISSN 2581-5369]

risk associated with authentication, malware, and verifiability is increased due to this subsequent technological breakthrough.

- Fourth, it will discuss the unique and subliminal threat of influencing the algorithms, how it can impact the voters.
- Finally, the paper will end with the conclusion, which proposes a holistic framework of reimaging and strengthening the electoral sovereignty of India in the digital age and taking a proactive and multi-stakeholder approach in protecting the most significant democracy in the world.

## II. HISTORICAL CONTEXT: THE ERA OF BOOTH CAPTURING AND REFORMS

1. **Booth capturing :**To comprehend the magnitude of the current digital challenge, it is essential to appreciate the victories won in the past. The early decades of independent India's electoral history were spoiled by practices that directly assaulted the principle of "one person, one vote." Booth capturing was the most flagrant malpractices that involved supporters of a candidate or party physically taking over a polling station, often through violence and intimidation, to cast a large number of false votes. It was especially endemic in areas where the state was weak, feudal, and had high political stakes e.g., Bihar, Uttar Pradesh and West Bengal. It was being done in a brazen manner: the polling officials would be overpowered, the real voters would be turned away, and ballot boxes would be stuffed with already marked ballot papers. This practice not only disenfranchised legitimate voters but also created an atmosphere of fear and this fundamentally undermined the freedom of the electoral process as well.[5]

Other analog threats that occurred in addition to booth capturing are:

a) Voter Intimidation: It involves keeping away certain communities or certain groups of people by threat of violence on their way to the polling points.

b) Rigging and Bogus Voting: Impersonation of absent or dead voters to vote more than once.

c) Violence/Muscle Power- The ability to win votes by creating a fear atmosphere with the help of local strongmen so that one could choose a certain candidate.

d) Abuse of State Machinery: The party who is in power makes use of government funds and resources and other governmental staff members to campaign and give an unfair

[5] Vaishnav, M. (n.d.). When Crime Pays : Money and muscles in Indian politics (2017th ed.).

 [ISSN 2581-5369]

playing field.

Article 324 of the Constitution of India gave the ECI the authority to embark on a process of comprehensive reform that in a systematic manner pulled down this structure of physical malpractice. These were administrative reforms and technological reforms. [6]

**Unveiling of Electronic Voting Machines (EVMs):** The EVM was a game-changer. It was used to replace the cumbersome and easily corrupt system of ballot papers. An EVM has a way of self-locking after voting and can only be reactivated by an officer who will be the poll. This mechanism constrains the amount of voting to a maximum of four or five votes in a minute and the cramming of ballots in tightly in a booth, which is characteristic of booth capturing, would be technically infeasible. The electronic trail of all the votes can also be obtained through the control unit of the EVM closely noting the order and time in which they were made.

**Voter Verifiable Paper Audit Trail(VVPAT):** To improve lingering suspicion about black box essence of the EVMs and to improve voter confidence, the ECI implemented VVPAT system. This machine, which is connected to the EVM, will print a slip on paper with a name and symbol of the selected candidate, which will last a few seconds in sight of the voter before being dropped into a closed box. This gives us a physical audit trail on which one can check the electronic count to add an important level of transparency and accountability.

**Elector Photo Identity Card (EPIC):** Introduced is the mandatory use of photo ID by the voters and this led to drastic reduction in the area of impersonation/ bogus voting. This was a very simple but effective measure since it served to make sure that only the registered voters had the chance to vote.

**Strict Implementation of the Model Code of Conduct (MCC):** The ECI started implementing the MCC with rigor and strictness as never before. This code of ethics controls how the political parties and candidates conduct themselves during this time, how they might seek to misuse the state machinery, how they may wish to give inflammatory speeches, and other unjust actions taken.

**Implementation of Central Security Forces:** In the quest to provide a neutral and secure environment to carry out the polling process, the ECI started the implementation of Central Armed Police Forces (CAPFs) in suspected constituencies. Under the direct command of the ECI, these forces served the purpose of neutralizing the influence of local politics and stopping voter intimidation.

[6] GOVERNMENT OF INDIA, & Shah, A. P. (2015). Electoral reforms. In *Report No.255*. https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2022/08/2022081635.pdf

 [ISSN 2581-5369]

By early 2000s, these measures were very successful. Cases of booth grabbing and massive rigging became minimal. The physical integrity of the ballot box had been sufficiently provided by the ECI. But the success could unwittingly make malafide actors turn to less conspicuous methods of driving electoral results.

## III. ELECTRONIC VOTING SYSTEMS IN INDIA MAY HAVE WEAKNESSES

Electronic voting systems in India are one of the probable vulnerabilities that have been researched by different investigators. The weakness of the electronic voting machines in India has been discovered through examinative studies. Such machines are prone to fraud and can be blamed as not being reliable. This may come as a weakness of electronic voting in India because third parties cannot be assured that the systems are subjected to any personal verification. The citizenry can not easily monitor the systems to identify any anomalies since the software source code employed to run the electronic voting machines is not readily available to them. The threat actors take advantage of the existing gaps in technology to breach and taint the democratic landscape, raising a point of serious concern on the nature of democracy itself. Other possible vulnerabilities that will come to compromise the integrity of the whole voting process are the hacking of the EVMs and interference with voting registration databases.

In addition, the Indian electronic voting machines have simple embedded system architecture, which is very different as compared to the elaborate voting machines in the US and Europe. Weaknesses of Indian electoral process are also visible since the political parties are making accusations of cheating and electoral violence in the outcome of the elections. The Indian authorities have never allowed strict and independent evaluation of the security of the electronic voting machines and this again underscores the security dangers that the electronic voting machines may pose in India. The issue of creating a voting system which gives both transparency and security is a challenge in India and other democracies since the research revealed that there are technical issues in the electronic voting system in India and it has implications on voting technology in India and other countries.

## IV. DIGITAL TRANSITION: NEW FIELDS OF ELECTORAL MANIPULATION

The social media, big data and ubiquitous connectivity defines the digital ecosystem which has become the new frontier of the electoral contest. The threats in this area are not the physical act of voting that needs to be controlled but the manipulation of the cognitive processes that lead to voting.

 [ISSN 2581-5369]

**1. Disinformation and Misinformation:** Poisoning the Well The biggest and most effective weapon of the digital era is the disseminated disinformation (deliberately false information) and misinformation (inadvertently published falsehoods). The social media networks such as Facebook, WhatsApp, and X (previously Twitter) have turned out to act as potent sources of such content.These media networks are meant to get the user as engaged as possible. Their algorithms give priority to sensational, emotionally charged and polarizing content due to the fact that it attracts more clicks, shares and comments. This provides fertile grounds of disinformation which in most cases is meant to be provocative. Consequently, fake stories may go viral and more rapidly than actual refutations.For example: - In 2016, the US presidential elections, a tweet about a supposedly rigged voting machine in Philadelphia was reposted over 11,000 times. Later on it was found out that the initial tweet was an error of a voter who had not followed the Instructions displayed on the voting machine.

Social media profiles, data brokers, and even data breaches now can be used in political campaigns to generate highly specific psychological profiles of voters using vast datasets. This will enable them to send personalized messages that aim at playing off of personal fears, prejudices, and tastes. To illustrate, a caste based appeal can be micro-targeted at a certain community within a certain constituency, without being noticed by the masses and the regulators. This dilutes the popular discourse and complicates the possibility to blame campaigns with divisive discourse. WhatsApp has more than 853.8 million users in India[7], making this a very powerful weapon of misinformation because it is end-to-end encrypted. This leaves the platform and the law enforcement unable to track the content that is shared on private groups. These groups are turned into echo chambers during election years where a flood of fake news and manipulated visuals and inflammatory videos are disseminated to agitate communal hatred, depress voter turnout among some groups, or create fake stories about candidates.

**2. Cyber-Attacks of Election Infrastructure:** The EVMs themselves are detached machines, and they are not connected to the network, but the overall electoral system is becoming digitalized, and thus prone to cyber-attacks. A high-value target is the electoral rolls that hold personal information of millions of citizens. Such data may be used to commit identity theft or even worse, micro-targeting or voter suppression could happen in a breach of this data. An example is that an attacker can use the database to remove or modify the records of the voters of a certain demographic, and result in carnage and disenfranchisement on polling day. Although the voter ID and Aadhaar linkage are aimed at cleaning up the voter lists, the websites

[7] Raj, H. (2025, April 22). *WhatsApp statistics for 2025 – All you need to know*. Verloop.io. https://www.verloop.io/blog/whatsapp-statistics-2025/

 [ISSN 2581-5369]

and applications of the ECI are the most important in terms of the information they provide to the voters, including the location of the polling stations, candidate affidavits and results. A DDoS attack has the potential to shut down these services at a very critical time causing confusion and loss of trust. False information posted on the ECI site could do the same destabilizing effect.Polling officials communicate through different communication networks to report polling data and logistical problems during the election day. Any disruption of these networks would affect the normal running of the election and slow down the relaying of the results.

**3. Third-party and Online Voting: Hope and Dangers.** The ECI is in the process of finding solutions to remote voting so that migrant workers, service voters and other citizens who cannot be physically present in their respective registered constituencies on polling day can be enfranchised. In 2023, it unveiled a prototype of a Remote Voting Machine (RVM) a multi-constituency EVM. Although the shift to any type of digital or distance voting is noble in nature, it provides a Pandora's box of fresh and increased dangers to electoral sovereignty. The in-person voting system has a physical, controlled environment; the polling booth, upon which the security of the existing system is based. It is overseen by the trained officials, checked by the party agents and guarded by the security forces. By definition, remote voting transfers the voting process to an uncontrolled, "trustless" platform, like a voter on his or her personal laptop or an external remote voting center. This essentially changes the security calculations. The question is raised that how will the system be sure that the individual casting the vote is the right voter and is not being forced to do so? Although biometrics (fingerprints, facial recognition) may be suggested as the solution, it is not infallible. The biometric information is spoofable and deepfake technology has a potential to defeat liveness checks in video authentication. What is more significant is that technology is unable to notice a family member or local strongman lurking out of camera, bullying the voter to make his/her choice. This is a re-creation of the voter intimidation, but this time, not at the polling point, but at the comfort of the voter at home. In case the voting is carried out through personal devices (smartphones, computers), the integrity of the vote depends on the security of the device. A malware'd device may modify or change the vote without the user's awareness (a so-called man-in-the-browser attack) or log the vote and breach the secrecy of the ballot. It is a realistic impossibility to guarantee the security of millions of different privately-owned devices.

The whole process would be based on the secure network connection to the central server. This provides numerous points of failure. The information in transit may be susceptible to interception or manipulation by man in the middle attacks. The voting system, which is stored

 [ISSN 2581-5369]

on the central servers, would be of a very high value to state-sponsored hackers, who could either seek to manipulate the vote counts, sabotage the election, or simply undermine the validity of the results by a successful intrusion.

**4. Verifiability-Anonymity Dilemma** is the core cryptographic and democratic challenge of remote voting. An ideal system must allow a voter to verify that their vote was recorded as cast and counted as recorded. At the same time, it must preserve the secrecy of their ballot to prevent coercion and vote-selling. These two requirements are in direct tension. Systems that provide strong verifiability (e.g., by giving the voter a cryptographic receipt) often risk compromising anonymity, and vice versa. Without a universally accepted and easily understandable solution to this problem, any remote voting system will struggle for public trust.
The push for remote voting, while well-intentioned, risks leapfrogging into a technological paradigm for which the security, legal, and social frameworks are not yet mature. A failed or compromised remote voting pilot could irreparably damage public faith in the entire electoral process.

## V. ALGORITHM MANIPULATION

It might be the most pernicious danger to electoral sovereignty, but the manipulation of the algorithms through which we live our digital life is so difficult to observe. This transcends the dissemination of fake news [8]and borders on the insidious methods by which political preferences can be biased in information settings in a manner that is practically invisible to those subjected to it.

**Search Engine Manipulation Effect (SEME)** The Research of psychologist Robert Epstein and others has shown that the placement of search results can be very influential in opinions and voting decisions of indecided voters. This is known as the Search Engine Manipulation Effect (SEME) which is one of the strongest behavioral effects that has ever been found.[9] A search engine company can, in principle, change the millions of votes without the knowledge of anyone by just rearranging search results so that they would prefer a particular candidate. The impact is also so high since users have confidence in the search results of organic search and they are also usually not aware of the ranking bias. Since one firm, Google, has a near-monopoly on search in India, the possibilities of biases deliberate and accidental are vast. This

[8] The Hindu Bureau. (2024, March 26). *Misinformation during Indian elections: The saga from 2019 to 2024*. The Hindu. https://www.thehindu.com/news/national/misinformation-during-indian-elections-the-saga-from-2019-to-2024/article67989996.ece

[9] Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences of the United States of America*, *112*(33), E4512–E4521. https://doi.org/10.1073/pnas.1419828112

is a direct menace to sovereignty whereby a foreign corporation may have the authority to influence a national election.

Social Media can also be algorithmically manipulated since the news feeds on Facebook and Instagram are not chronological or neutral, but rather the algorithmically edited list of content that the site thinks the user will be interested in. This forms filter bubbles and echo chambers whereby people are mostly exposed to information that supports their pre-existing beliefs. In the long run, it may cause the situation of greater political polarization and the inability to engage in cross-ideological dialogue. These algorithms could be used during an election to provide entirely distinct realities to various groups of voters and a shared basis of democratic discussion could not be found.

The manipulation of the algorithms is subtle in nature and this is the defining feature. There is no evident case of a crime, as there is in an apprehended booth or a hacked web site. The manipulation is concealed in proprietary code and the manipulation would be virtually impossible to be detected or proven by outsourced auditors or regulators. This is an extreme lack of transparency to democratic responsibility.

## VI. NEEDED FRAMEWORK FOR THE DIGITAL AGE

The shift to online threats also demands a corresponding change in how we treat the problem of electoral security. The multi-stakeholder need of this new era is to protect the electoral sovereignty of India.

a) **Legislative and Regulatory Revamp**: The first line of defense is having a well built data protection law that is stronger than the existing Digital **Personal Data Protection Act 2023**. [10]The legislation should put a very strict restriction on how political parties should gather, process, and utilize the personal data of the voters and campaigning, and if not then, there should be very serious consequences.Social Media Platforms should have a greater responsibility to the content they will spread. This might include requirements of more transparency in their content moderation policies and algorithms, prominent labelling of political advertisements and their sponsors, and more robust requirements to collaborate with the ECI taking down provable false and malicious content during elections.The Representation of the People Act, 1951[11], should be

[10] Parliament. (2023). THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023. In *THE GAZETTE OF INDIA EXTRAORDINARY*. https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf

[11] Government of India. (1951). THE REPRESENTATION OF THE PEOPLE ACT, 1951. In *THE REPRESENTATION OF THE PEOPLE ACT, 1951*. https://www.indiacode.nic.in/bitstream/123456789/2096/5/a1951-43.pdf

 [ISSN 2581-5369]

changed to explicitly specify and penalize the new types of electoral malpractices that are digital impersonation, malicious use of AI to create malicious deepfakes, and coordinated disinformation.

b) **Technological Barrier and Institutional Capacity Building:** The ECI should ensure that it has a permanent, well-endowed cybersecurity wing with the best technical experts .This unit would be mandated with the role of carrying out constant surveillance of the electoral infrastructure, gathering of threat intelligence, making consistent audits of all digital systems, coordinating response to cyber-incidents. The ECI needs to add greater collaboration with the other national organizations such as CERT-In (the Indian Computer Emergency Response Team), the National Critical Information Infrastructure Protection Centre (NCIIPC) and even hackers to actively find out their vulnerability. Any step towards remote or online voting will have to be accompanied by widespread consultation to the population, a high-quality independent security testing of the suggested technology, and the creation of a complete legal framework. Security by design must be a principle, and not something that follows.

c) **Empowering the "Human Firewall": The Role of the Electorate -**Nationwide Digital and Media Literacy is the single most effective long-term defense against disinformation is an informed and critical citizenry. The government and civil society must invest heavily in large-scale digital literacy programs, starting from the school level. These programs should teach citizens how to identify fake news, understand the basics of online privacy, and recognize manipulative content. Supporting independent, non-partisan fact-checking organizations is crucial. The ECI could partner with such organizations to quickly debunk false claims during elections and disseminate clarifications through its own communication channels.

d) International Cooperation Digital threats, especially those related to state-sponsored actors, are a global menace. India ought to take the center stage in establishing international rules and agreements over non-interference in election by use of cyber means. This is by exchanging best practices and threat intelligence with other democracies that are experiencing challenges.

## VII. CONCLUSION

The history of Indian election since the days of booth capturing up to algorithm manipulation is evidence of its strength and its changing weaknesses. The achievement of the ECI to sanitize the physical process of voting was an achievable milestone that ensured the machinery of

democracy. The sanctity of an election however is not necessarily a mechanical process but a cognitive and social process. These days, the attack is on voter minds, the information integrity, and even the structure of the trust that people have.

The disinformation, computer-attacks, and the insidious influence of algorithms are much more complicated than their analogs. They are anonymous, are hard to trace, and are active in the legally gray zone of the digital space. The suggested transition to remote voting, unless approached with extreme care, will add many new attack points exponentially.

The restoration of electoral sovereignty of India in the 21 st century is not merely the work of the Election Commission. It needs a societal level response. It needs a legislature that is responsive enough to control the fast evolving technological environment. It demands technology platforms to carry their rigorous civic obligations. It needs a strong civil society and media that is keen in their capacity as truth-tellers. Most importantly it needs an electorate which has the critical thinking capability to wade through a polluted information ecosystem.It is no longer a matter of defending the ballot box, but is the democratic mind itself that needs to be defended. India has demonstrated the ability to be democratic in the innovation in the past. It has to do it again in order to protect its future.

*****

 [ISSN 2581-5369]

## VIII. REFERENCES


- Wikipedia contributors. (2025, March 15). *Electronic voting in India*. Wikipedia. https://en.wikipedia.org/wiki/Electronic_voting_in_India
- Vaishnav, M. (n.d.). When Crime Pays : Money and muscles in Indian politics (2017th ed.).
- Varshney, A. (n.d.). *"Democracy at gunpoint."*
- Sridharan, E., & Vaishnav, M. (2017). Election Commission of India. In *Oxford University Press eBooks*. https://doi.org/10.1093/oso/9780199474370.003.0011
- GOVERNMENT OF INDIA, & Shah, A. P. (2015). Electoral reforms. In *Report No.255*. https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2022/08/2022081635.pdf
- The Hindu Bureau. (2024, March 26). *Misinformation during Indian elections: The saga from 2019 to 2024*. The Hindu Newspaper
- Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. Proceedings of the National Academy of Sciences, 112(33), E4512-E4521.
- **Election Commission of India** – History of Reforms in Indian Elections.
- Election Commission of India (ECI). (2021). EVM & VVPAT: Status Paper. Retrieved from [ECI Official Website].
- Venkatesan, V. (2009). The curse of booth-capturing. Frontline, 26(09).
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146-1151.
- Seshia, S. A., et al. (2021). Securing the Vote: A Report of the National Academies of Sciences, Engineering, and Medicine. The National Academies Press.
- Carnegie Endowment for International Peace. (2019). India's 2019 Elections: The Role of Social Media.
- Observer Research Foundation (ORF). (2022). Cybersecurity and India's Elections: Preparing for 2024.
- The Representation of the People Act, 1951.


 [ISSN 2581-5369]

- Digital Personal Data Protection Act, 2023.


*****

 [ISSN 2581-5369]