IRHAMNA
International Research of Sustainability Management, Business, & Administration
Volume 1, Number 1, 2025 pp. xx-xx
E-ISSN : XXXX-XXX

Supervision Without Enforcement: Preventing Social Media Campaign Violations in Indonesia's 2024 Regional Elections

Kurhayadi[1*], Edi Iskandar[1], Somantri[1], Susila[1], Temban Joshua Temban[2]

1 Program Studi Ilmu Administrasi Negara, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Al-Ghifari, Bandung, Indonesia
2 University of Buea, Buea, Southwest Region, Cameroon

1 kurhayadi@unfari.ac.id

Article History

Received :
Revised :
Accepted :

ABSTRACT

Social media has become the main arena for local election campaigns and a major channel for hate speech, hoaxes, and content that exploits ethnic and religious divisions. This study examines the strategies a provincial election supervisory body used to prevent campaign violations on social media, the challenges it faced, and its responses. We conducted a qualitative single case study of the Election Supervisory Body (Bawaslu) of West Java during the 2024 gubernatorial election, guided by Koteen's typology of public organization strategy. Data came from interviews with six secretariat staff, observation of online campaigning, and cyber-monitoring documents. By 19 November 2024, the body monitored 730 official accounts of candidates and campaign teams and recorded 181 violations, most of them on TikTok. Organizational strategy simply followed national regulations and circulars. Programme strategy relied on daily cyber patrols of registered candidate accounts and educational content. Resource strategy compensated for shortages of staff, facilities, and budget through help from other units and student interns. Institutional strategy consisted of cooperation with national and provincial agencies. Bawaslu could not take down accounts or content and could only forward findings to the ministry. We propose the concept of supervision without enforcement and show that monitoring centred on official accounts misses anonymous accounts, the main locus of violations. Priority-flagger status with platforms and permanent cyber-monitoring staff would strengthen supervision. All informants came from the provincial secretariat, which limits the range of perspectives.

Keywords: Election Supervision; Digital Campaigning; Platform Governance; Public Organization Strategy; Electoral Integrity

Available Online: https://doi.org/10.38043/irhamna.v7i2.3799

This is an open access article licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

INTRODUCTION

Direct elections of regional heads are a central feature of local democracy in Indonesia. Their integrity depends not only on polling day but also on the quality of the campaign. Norris (2014) shows that violations of electoral integrity can occur at every stage of the electoral cycle, including the campaign, and that such violations erode citizens' trust in democratic processes. In the digital era, more and more of the campaign takes place on social media. Garnett and James (2020) note that digital technology offers opportunities to election administrators but also poses new threats to electoral integrity, including the spread of false information online. Wardle and Derakhshan (2017) describe this condition as information disorder, an ecosystem in which misinformation, disinformation, and malicious information circulate and

* Corresponding Author: Kurhayadi: kurhayadi@unfari.ac.id

reinforce one another. Protecting the integrity of elections is part of the broader goal of building accountable and inclusive institutions under Sustainable Development Goal 16 (United Nations, 2015).

In Indonesia, campaigns that insult individuals, religions, ethnic groups, races, social groups, candidates, or political parties, and campaigns that incite, slander, or pit groups against one another, are prohibited by Article 69 of Law No. 1 of 2015 on the Election of Governors, Regents, and Mayors and its amendments. For electronic content, Law No. 1 of 2024, the second amendment to the Electronic Information and Transactions Law, prohibits the distribution of information that incites hatred based on identity and of false information that causes unrest, and it gives the government the power to cut off access. Supervision of compliance by election participants is the task of the Election Supervisory Body (Badan Pengawas Pemilihan Umum, Bawaslu) and its hierarchy.

The difficulty is that campaign violations on social media are committed not only by candidates, political parties, or official campaign teams, but also by individuals and groups that are not registered as part of any campaign. Public data from West Java illustrate the problem sharply. The chair of Bawaslu West Java stated that among the 720 official accounts of election participants under supervision, no violations had been found by the end of vote counting, while anonymous accounts and paid amplifiers (buzzers) remained widespread on social media (Prayoga, 2024). At the same time, cyber monitoring recorded 192 findings, mostly hate speech and hoaxes on TikTok, all of which were referred to the Ministry of Communication and Digital Affairs (Prayoga, 2024).

Indonesian studies of election supervision on social media have so far been largely descriptive. Karim (2023) described the strategy of Bawaslu East Java in the 2019 general election, which involved collaboration with influencers, discussion forums, and the integrated law enforcement centre. Afnira (2023) examined the use of social media to publicize supervision by Bawaslu in Tanjungpinang. In a literature review, Putri et al. (2024) found that Bawaslu's reporting application supported public participation, but that supervision was constrained by limited personnel, the speed at which information spreads, anonymous accounts, and weak protection for whistle-blowers. Husaini et al. (2024) discussed Bawaslu's role in addressing election violations in the digital era from the perspective of Law No. 7 of 2017. These studies mostly focus on national elections and list activities. They have not yet related supervision strategies to the structural problem of how authority is divided among election supervisory bodies, the government, and digital platforms.

This article addresses that gap with three questions: (1) what strategies did a provincial election supervisory body use to prevent campaign violations in regional elections on social media; (2) what challenges did it face; and (3) what measures did it take to address those challenges? Using Koteen's typology of public organization strategy as presented by Salusu (1996), and placing it within the literatures on electoral governance and platform governance, we argue that provincial prevention strategies were shaped by two gaps: a gap between the mandate to supervise and the power to enforce, and a gap between the target of supervision (official accounts) and the locus of violations (unofficial accounts). The conceptual contribution of the article is the notion of supervision without enforcement as a way of reading the position of election supervisory bodies within regimes of digital content governance. The article first reviews the literature, then describes the policy context and methods, presents and discusses the findings, and concludes with suggestions for future research.

LITERATURE REVIEW

Electoral Governance and Integrity in the Digital Era

Mozaffar and Schedler (2002) distinguish three levels of electoral governance: rule making, rule application, and rule adjudication. Supervisory bodies such as Bawaslu work mainly at the level of rule application, ensuring that participants and administrators comply with the rules of the game. This framework is useful because it shows that the effectiveness of supervision depends on what happens after a violation is detected, that is, on whether there is a mechanism able to enforce the rules.

Norris (2014) understands electoral integrity as compliance with international norms across the electoral cycle, from the legal framework and campaign to media coverage and vote counting. Garnett and James (2020) add that digitalization shifts part of the threat to electoral integrity into cyberspace, including disinformation campaigns, and requires election bodies to develop new capacities. Wardle and Derakhshan (2017) stress that information disorder involves agents, messages, and interpreters, so that responses cannot focus on a single type of actor. Tenove (2020) adds a normative caution: policy responses to disinformation can themselves threaten democratic goods such as free expression if they

give state bodies broad powers over content. Any proposal to strengthen election supervision online must therefore weigh effectiveness against the risk of overreach.

Platform Governance

Gorwa (2019) defines platform governance as the layers of relationships between platforms, users, advertisers, governments, and other political actors that determine how content is regulated. In this arrangement, the real power to remove content rests with platforms and, in some regimes, with governments that can order platforms to act. Other bodies, including election administrators, can usually only flag content and request action. Platforms are not passive in elections. Kreiss and McGregor (2018) show that technology firms work closely with campaigns and actively shape political communication, which means that platforms already maintain channels with political actors when it suits them. The European Union has institutionalized a stronger position for certain reporters through the status of trusted flagger under the Digital Services Act, whose notices platforms must process with priority (Regulation (EU) 2022/2065). The comparison matters because it shows that the position of a reporter can be strengthened institutionally rather than left as ordinary reporting.

Public Organization Strategy

Salusu (1996), drawing on Koteen, distinguishes four types of strategy in public and non-profit organizations. *Organizational strategy* concerns the formulation of mission, goals, values, and new strategic initiatives. *Programme strategy* concerns the strategic implications of a given programme. *Resource support strategy* concerns the optimal use of staff, funds, technology, and assets. *Institutional strategy* concerns the development of the organization's capacity to carry out strategic initiatives. The four types are often read as a hierarchy. In a multi-level organization such as Bawaslu, the typology raises an empirical question: how much room does a provincial unit actually have to formulate strategy, rather than merely carry out a strategy set at the centre?

Collaborative Governance

When one agency lacks the authority and resources to deal with a problem, collaboration across agencies becomes an option. Ansell and Gash (2008) show that the success of collaborative governance depends on starting conditions, including imbalances of power and resources among the parties, institutional design, facilitative leadership, and a collaborative process that builds trust and shared understanding. We use this framework to read Bawaslu's cooperation with other agencies, focusing on whether such cooperation adds to enforcement capacity or merely widens the reporting network.

Analytical Framework

The study uses Koteen's four strategy types as descriptive categories to map the strategies of the provincial body. The findings are then read through two lenses. The first, drawn from the literatures on electoral and platform governance, asks where the power to enforce lies. The second, drawn from the literature on information disorder, asks whether the target of supervision matches the source of violations. Challenges and measures are analyzed as the relationship between these two lenses and organizational capacity.

MATERIALS AND METHODS

Policy Context

The main legal basis for regional elections is Law No. 1 of 2015 on the Election of Governors, Regents, and Mayors, last amended by Law No. 6 of 2020. Article 69 of the law sets out the campaign prohibitions noted above. Bawaslu's status as a permanent supervisory body with branches at provincial and district levels is set out in Law No. 7 of 2017 on General Elections, and supervision of the 2024 regional elections is further regulated by Bawaslu Regulation No. 6 of 2024.

For the online sphere, the national Bawaslu issued Circular No. 102 of 2024 on the Prevention of Violations and Supervision of Internet (Cyber) Content in the 2024 Elections. According to documents collected for this study, the circular instructed provincial and district bodies to form cyber content supervision facilitation teams. These teams were to identify the risk of hoaxes; carry out collaborative prevention with stakeholders including communication and informatics agencies, the police cyber unit, civil society organizations, election monitors, social media platforms, and the media; identify violating accounts and content; coordinate with the level above when content lay outside their jurisdiction; provide

online and offline electoral literacy education; and publicize official channels for complaints about the exploitation of ethnic and religious issues, hoaxes, and hate speech.

The power to cut off access does not lie with Bawaslu. Article 40(2b) of Law No. 1 of 2024 provides that the government may cut off access or order electronic system operators to do so. During the 2024 campaign period, the ministry in charge changed from the Ministry of Communication and Informatics (Kominfo) to the Ministry of Communication and Digital Affairs under Presidential Regulation No. 174 of 2024, issued on 5 November 2024. We use the name used by informants (Kominfo) when quoting them.

West Java has a very large electorate; the research documents record a final voter list of 35.9 million for the 2024 gubernatorial election. The secretariat of Bawaslu West Java is classified as a class A secretariat on the basis of its workload. It is headed by a senior official at echelon II level and is administratively accountable to the Secretary General of Bawaslu and functionally accountable to the chair of the provincial Bawaslu.

Research Design and Informants

We used a qualitative approach with a single case study design (Yin, 2018). The case is Bawaslu West Java, based in Bandung, during the 2024 gubernatorial election. The case was chosen because of the size of the electorate and the intensity of social media campaigning, which made the pressure on cyber-monitoring capacity clearly visible.

Informants were selected purposively according to their involvement in supervising and preventing campaign violations. All came from the secretariat of Bawaslu West Java (Table 1) and are identified by code.

Table 1. Research informants

Code	Position	Unit
I1	Public relations officer (junior expert)	Legal, Public Relations, Data and Information Division
I2	Public relations officer (first expert)	Legal, Public Relations, Data and Information Division
I3	Head of Supervision Division	Supervision Division
I4	Head of Administration Division	Administration Division
I5	Supervision staff	Supervision Division
I6	Bawaslu functional officer	Provincial Bawaslu

Source: research data, 2025.

Data Collection and Analysis

Primary data were collected through in-depth interviews with a semi-structured guide organized around Koteen's four strategy types, challenges, measures, and regulations, and through observation of social media campaigning during the 2024 gubernatorial campaign period. Secondary data consisted of cyber-monitoring documents of Bawaslu West Java, including the recapitulation as of 19 November 2024, Circular No. 102 of 2024, and relevant laws and regulations. Interviews were conducted in Indonesian, and the excerpts below were translated by the authors.

Analysis followed the stages of data condensation, data display, and conclusion drawing and verification (Miles et al., 2014), combined with thematic analysis (Braun & Clarke, 2006). Initial coding used Koteen's four strategy types as deductive categories, while themes on challenges and measures were developed inductively from the data. The credibility of the findings was supported by triangulation across informants and across techniques (interviews, observation, and documents).

The third author completed an internship at Bawaslu West Java from September to December 2024. This position eased access to informants and documents, but it may also have affected how informants answered and how the data were interpreted. To limit this influence, interview accounts were checked against documents wherever possible, and discrepancies between sources, such as differences

between figures in the recapitulation and in public statements, are reported rather than reconciled. Informants took part voluntarily after being told the purpose of the study, and their names are withheld.

RESULTS AND DISCUSSION

The results are organized by Koteen's four strategy types, followed by the challenges and measures. The discussion then reads the findings through the two analytical lenses.

Overview of Social Media Campaign Supervision

According to the cyber-monitoring report of Bawaslu West Java as of 19 November 2024, 730 official accounts of election participants and campaign teams were monitored on Instagram, Facebook, TikTok, YouTube, and Twitter, together with the monitoring of hashtags and keywords. Monitoring and cyber complaints, covering both social media platforms and news portals, recorded 181 violations, including 151 instances of hate speech and 37 hoaxes. TikTok was by far the dominant platform, with 178 violations, while the rest were spread across other platforms. The categories of hate speech and hoaxes together (188) exceed the reported total (181), and the source document does not explain the difference; one item may have been classified under more than one category.

Organizational Strategy

Informants described organizational strategy as the implementation of central regulations. I1 explained:

> *"Our organizational strategy for preventing or supervising campaign violations on social media, especially in the 2024 regional elections, refers to the circular issued by the national Bawaslu, under which we have the authority to supervise or prevent campaign violations and to report the results of supervision step by step from the district Bawaslu up to the national Bawaslu." (I1)*

I2 said the same more briefly:

> *"Bawaslu only carries out the regulations of the national Bawaslu on preventing and supervising the campaign during the election stages." (I2)*

I6 stressed that the provincial level had no room for its own formulation:

> *"Actually the provincial Bawaslu has no internal regulations. The provincial or district Bawaslu only carries out what the centre has formulated. The regulations from the centre are passed down as a reference or guideline for supervising and preventing violations during the election stages." (I6)*

The organizational strategy of Bawaslu West Java was therefore not autonomous. The provincial body acted as an implementer of central policy, with an emphasis on regulatory compliance, vertical coordination, and tiered reporting from districts up to the national Bawaslu.

Programme Strategy

Programme strategy had two components: cyber monitoring and public education. I1 described the monitoring mechanism:

> *"In our programme strategy we formed a cyber supervision facilitation team whose task is to monitor the accounts of candidates registered with the Election Commission. This is done through daily cyber patrols throughout the campaign period. The Bawaslu team monitors directly in cyberspace, and the results are reported step by step, starting from the district level, then the province, and finally the national Bawaslu. If indications of a violation require follow-up, the report is forwarded to the Ministry of Communication and Informatics. [...] Our efforts include educational content on Instagram about campaign rules and invitations to keep social media ethics. We also make digital posters and spread them across social media platforms to raise public awareness." (I1)*

I2 named the types of violations targeted:

> *"At Bawaslu there is cyber supervision, which monitors the accounts of candidate pairs registered with the Election Commission. The campaign violations include hate speech, false news, and content involving ethnic, religious, and racial issues. To prevent violations, we make educational content about the election, its rules, and campaign ethics." (I2)*

I5 from the Supervision Division pointed to an internal division of labour between offline and online prevention:

> *"In the Supervision Division, prevention is mostly about direct contact with the public, like outreach, supervision corners, supervision villages, and so on. For social media, the responsibility lies with the Legal, Public Relations, and Data and Information Division, which formed the social media supervision facilitation team with members from all divisions, called cyber supervision, to monitor*

campaign violations in the digital sphere. For prevention, that division makes educational content in collaboration with student interns, and all internal units take part in supervision." (I5)

Programme strategy thus combined daily cyber patrols of registered candidate accounts, tiered reporting that ended in referral to the ministry, educational content and digital posters, and face-to-face outreach through supervision corners and supervision villages. The patrol targets named by informants were the official accounts of candidates.

Resource Support Strategy

All informants asked about resources said that they were still limited. I1 explained:

"In terms of resources we are still limited, especially in human resources. The wide scope of supervision often overwhelms the team. But this can be overcome with help from various parties, including support from other units within Bawaslu and the participation of student interns in cyber supervision shifts. To optimize supervision, Bawaslu also cooperates with various institutions, such as Kominfo, the National Cyber and Crypto Agency, and the district Bawaslu." (I1)

Limitations also concerned facilities and the budget for producing content:

"Resources are still lacking at the moment, and so are facilities. For example, in making content we still use whatever is available, and the centre has no regulation yet on a special budget for it." (I2)

I6 pointed to a limitation of authority rather than capacity alone:

"The West Java Bawaslu does not have IT that can take down violating accounts. This is still difficult, and Bawaslu has no authority to act directly against violating accounts. To increase supervision capacity, Bawaslu West Java holds integrated training for the election supervision team." (I6)

Resource strategy was thus compensatory. Staff shortages were covered by other units and student interns, shortages of facilities and budget were covered by making do with what was available, and the absence of enforcement powers was covered by reporting to the authorities that had them.

Institutional Strategy

Institutional strategy took the form of a network of external and internal cooperation. I1 described it as follows:

"Bawaslu West Java cooperates with various related institutions. One form is cooperation with the National Cyber and Crypto Agency to improve monitoring and the handling of potential violations in cyberspace. Supervision is also strengthened by the sub-district election committees and district Bawaslu, which take an active part in cyber patrols and tiered reporting. We also cooperate with the provincial communication and informatics office and Jabar Saber Hoaks to coordinate the handling of hoaxes and campaign violations in digital media. This cooperation is formalized through a joint agreement, which is the basis for supervision and follow-up of violations. And we are also helped by student interns in cyber supervision, in making content, and in managing Bawaslu's social media." (I1)

"We cooperate with Bawaslu's internal units, and we also cooperate with Jabar Saber Hoaks in supervising social media." (I2)

"Bawaslu West Java also collaborates with various parties in supervision and prevention. For prevention, it works with student interns to manage social media and make educational content about the election to improve public understanding." (I6)

Externally, the partners named were the National Cyber and Crypto Agency, the provincial communication and informatics office, and the provincial government's anti-hoax unit, on the basis of a joint agreement. Internally, cooperation involved district Bawaslu, sub-district committees, other units of

the secretariat, and student interns. No informant mentioned direct cooperation with social media platforms, even though Circular No. 102 of 2024 lists platforms among the partners for prevention.

Table 2. Strategies to prevent campaign violations on social media

Strategy type	Forms found	Note
Organizational	Implementation of national circulars and regulations; tiered reporting	No provincial internal regulation
Programme	Cyber supervision team; daily patrols of registered candidate accounts; educational content and digital posters; supervision corners and villages	Patrols target official accounts
Resource support	Help from other units; student interns on cyber shifts; cooperation with Kominfo, the cyber agency, and district Bawaslu; training	Limited staff, facilities, and content budget; no power to take down accounts
Institutional	Cooperation with the cyber agency, provincial communication office, and anti-hoax unit through a joint agreement; support from district and sub-district bodies	No direct cooperation with platforms mentioned

Source: research data, 2025.

Challenges and Measures

The analysis identified five challenges and the measures taken in response (Table 3). The first challenge was limited human resources: the number of supervisors did not match the size of the territory and the intensity of campaigning on social media, and digital monitoring expertise was scarce. The second was limited facilities and budget for producing educational content. The third was limited authority, since Bawaslu could not act against or take down accounts directly. The fourth was the spread of hate speech and hoaxes faster than they could be handled. The fifth was limited public awareness of campaign rules on social media and low digital literacy, including low public participation in reporting violations.

Table 3. Challenges and measures in preventing campaign violations on social media

Challenge	Measures taken
Limited human resources	Student interns on cyber supervision shifts; help from other units; training for the supervision team
Limited facilities and budget	Producing educational content with available means, helped by student interns
Limited authority	Tiered reporting and referral of findings to the ministry; cooperation with the cyber agency, provincial communication office, and anti-hoax unit
Spread of hate speech and hoaxes	Daily cyber patrols by the supervision facilitation team
Limited public awareness	Educational content on Instagram and digital posters; outreach through supervision corners and villages

Source: research data, 2025.

Most measures extended existing strategies rather than changing the roots of the challenges. The response to limited authority, for example, consisted of reporting and cooperation, which did not change the fact that the final decision on violating accounts lay outside Bawaslu.

Supervision Without Enforcement

The most consequential finding of the study is that the supervision chain of the provincial body ended in referral. Cyber patrols detected, the team recorded, reports moved up the hierarchy, and findings were forwarded to the ministry. Article 40(2b) of Law No. 1 of 2024 places the power to cut off access with the government, and in practice the removal of content also depends on platforms. In the terms of Mozaffar and Schedler (2002), Bawaslu performs rule application, but for violations on social media this function is cut off from effective enforcement instruments. We call this position supervision without

enforcement: the supervisory body holds the mandate and the information, but not the lever that stops the violation.

The concept explains why the resource and institutional strategies we found were compensatory. When enforcement is unavailable, the organization multiplies detection and widens its reporting network. Gorwa (2019) shows that in platform governance, actors other than platforms and governments can usually only flag content. The comparison with trusted flagger status under the Digital Services Act shows that the flagging position can be institutionalized so that reports receive priority. Kreiss and McGregor (2018) show that platforms already work closely with official campaigns, which suggests that a direct channel between platforms and election bodies is feasible. In West Java, however, no informant mentioned a direct relationship with platforms, so Bawaslu's reports depended on a ministry as intermediary. In a short campaign period, every additional link lengthens the time between detection and removal.

The Gap Between Supervision Targets and the Locus of Violations

Informants named the targets of cyber patrols as the accounts of candidates registered with the Election Commission. This design follows the logic of election law, which regulates participants and official campaign teams. Yet the very background of this study is that violations are also committed by individuals and groups not registered with any campaign. Public data confirm this. The chair of Bawaslu West Java stated that no violations were found among 720 official accounts by the end of vote counting, while anonymous accounts and buzzers remained widespread, and 192 cyber findings were dominated by hate speech and hoaxes on TikTok (Prayoga, 2024). The figures in this study as of 19 November 2024 (730 accounts monitored, 181 violations, 178 on TikTok) are a recapitulation at a different point in time and are therefore not identical, but the pattern is the same.

In other words, programme strategy was designed for the actors who are easiest to regulate and least likely to violate rules openly, while violations moved to accounts that have no formal legal relationship with participants. Wardle and Derakhshan (2017) remind us that information disorder must be understood in terms of agents, messages, and interpreters. Supervision centred on official accounts touches only one type of agent. This is not a failure of implementers but a consequence of a legal framework that binds participants but reaches informal actors only through general criminal law and the access-blocking regime.

Strategy at the Provincial Level: Implementer, Not Formulator

Koteen's typology assumes an organization that formulates its own mission and strategic initiatives. The findings on organizational strategy show that at the provincial level this type is almost empty: informants stated that the province had no internal regulations and only carried out central formulations. The strategic room of the provincial body lay in the other three types, namely how to run programmes, how to patch resources, and how to build networks. For research on public organization strategy, this suggests that Koteen's hierarchy should be read in layers in multi-level organizations, with organizational strategy formulated at the centre and regional units operating within operational strategy. Studies that simply tick off all four types for regional units risk overstating their strategic autonomy.

Patched Capacity: Interns and Collaboration

Student interns appeared repeatedly in the data, in cyber supervision shifts, in producing educational content, and in managing Bawaslu's social media. This reflects organizational creativity under constraint, but also vulnerability. Interns are temporary, depend on the academic calendar, and do not build lasting institutional expertise. Garnett and James (2020) emphasize that cyber threats to electoral integrity require permanent technical capacity within election bodies. Reliance on temporary staff for core cyber-monitoring functions risks losing that capacity whenever an election ends.

Cooperation with the cyber agency, the provincial communication office, and the anti-hoax unit can be read through the framework of Ansell and Gash (2008). The starting conditions were marked by an imbalance of authority, since some partners had technical capacity or access to central government that Bawaslu lacked. The joint agreement provided a formal institutional design, but the data do not show whether the cooperation sped up follow-up on findings. Collaboration that widens the reporting network without shortening response times does not necessarily add enforcement capacity.

Education as Prevention: Reaching the Interpreters

The educational component of programme strategy deserves separate attention, because it is the only element that addresses what Wardle and Derakhshan (2017) call the interpreters of information disorder. Patrols act on accounts, and referral acts on content, but educational posts and offline outreach act on the voters who receive and share campaign messages. In principle, this component reaches the

space that official-account monitoring cannot, since it aims to make users less likely to spread hate speech and hoaxes regardless of who posted them.

In practice, the component was constrained in the same way as the others. Content was produced with whatever means were available, with no dedicated budget, and largely by student interns. Its reach was not measured, and informants described public awareness of campaign rules and willingness to report violations as low. Putri et al. (2024) made a similar observation about public participation in Bawaslu's reporting channels. Education therefore remained a modest complement to monitoring rather than a strategy in its own right. Given that violations concentrated on a single platform, TikTok, educational content tailored to that platform's formats and audiences may offer a more targeted route than general posters, although the present data do not allow this to be tested.

Policy Implications

First, the election legal framework should give Bawaslu a priority reporting channel to platforms, comparable to trusted flagger status, with clear response deadlines during campaign periods. Second, cyber supervision should be extended from official accounts to the networks of accounts that spread campaign content, under protocols that respect freedom of expression. Tenove's (2020) warning about normative threats is relevant here, since a body that monitors anonymous accounts must be bound by clear criteria and oversight. Third, the national Bawaslu should provide a dedicated budget for educational content and cyber supervision, since informants stated that no central regulation on this existed. Fourth, cyber supervision should be staffed by permanent personnel with social media analysis skills, with student interns as support rather than mainstay. Fifth, cooperation with regional partners should be evaluated by follow-up times rather than by the number of agreements signed.

Theoretical Implications

The concept of supervision without enforcement contributes to the electoral governance literature by locating the weakness of digital campaign supervision in the separation of rule application from enforcement, rather than in implementers' effort. It contributes to the platform governance literature by showing how a public body with a statutory mandate can still occupy the position of an ordinary flagger. And it qualifies the use of Koteen's typology in multi-level public organizations, where regional units implement strategies formulated elsewhere.

CONCLUSION

The strategies of Bawaslu West Java to prevent campaign violations on social media in the 2024 gubernatorial election can be mapped onto Koteen's four strategy types, but their weight was uneven. Organizational strategy followed the national Bawaslu entirely. Programme strategy relied on daily cyber patrols of official accounts and on educational content. Resource and institutional strategies served to patch shortages of staff, facilities, budget, and authority through help from other units, student interns, and cooperation with other agencies. The main challenges were limited resources, the lack of power to take down content, the rapid spread of hate speech and hoaxes, and low public awareness.

We conclude that the problem of supervising digital campaigns at the provincial level lies less in a shortage of activity than in two structural gaps: the supervisory body has no enforcement power over content, and its targets do not match the locus of violations. The concept of supervision without enforcement offers a way to read the position of election supervisory bodies in platform governance and points to reforms more specific than simply adding staff or outreach.

SUGGESTION FOR FUTURE RESEARCH

The study has several limitations that suggest directions for further research. All informants came from the secretariat of Bawaslu West Java, so the views of the provincial Bawaslu leadership, district supervisors, the ministry, platforms, campaign teams, and the public were not explored. Although six informants were interviewed, quotations were available from four of them, and the views of the heads of the Supervision and Administration divisions are not documented directly. Future studies should include the actors at the other end of the referral chain, especially the ministry and platforms, to establish what happens to findings after they leave the supervisory body.

The quantitative monitoring data come from a single recapitulation as of 19 November 2024 and contain an inconsistency between the total and its breakdown. The study also did not measure prevention outcomes, such as the number of items actually removed or the time taken to act on them, and therefore cannot assess the effectiveness of the strategies. Research that traces findings from detection to removal would allow the cost of supervision without enforcement to be measured directly. Comparative research across provinces, and between elections held before and after any reform of reporting channels, would

show whether priority reporting shortens response times. Finally, the third author's internship at the body studied may have made informants less critical; future studies by researchers without such ties would provide a useful check.

CO-AUTHOR CONTRIBUTION

The authors declare no conflict of interest in this article. All authors contributed to the conception and design of the study, the analysis and interpretation of the data, and the writing and revision of the manuscript, and all authors approved the final version.

ACKNOWLEDGEMENTS

The authors thank the secretariat of Bawaslu West Java Province for its cooperation. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. The authors used a generative AI tool to assist with restructuring and language editing. All data, analyses, and references were checked by the authors, who take full responsibility for the content.

Afnira, E. (2023). Optimalisasi media sosial sebagai sarana publikasi pengawasan Pemilu 2024: Kasus Bawaslu Kota Tanjungpinang [Optimizing social media to publicize supervision of the 2024 election: The case of Bawaslu Tanjungpinang]. *Jurnal Mahasiswa Komunikasi Cantrik*, *3*(1). https://doi.org/10.20885/cantrik.vol3.iss1.art4

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543–571. https://doi.org/10.1093/jopart/mum032

Badan Pengawas Pemilihan Umum Republik Indonesia. (2024). *Surat Edaran Nomor 102 Tahun 2024 tentang Pencegahan Pelanggaran dan Pengawasan Konten Internet (Siber) dalam Pemilihan 2024* [Circular No. 102 of 2024 on the prevention of violations and supervision of internet content in the 2024 elections]. Unpublished document.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Garnett, H. A., & James, T. S. (2020). Cyber elections in the digital age: Threats and opportunities of technology for electoral integrity. *Election Law Journal: Rules, Politics, and Policy*, *19*(2), 111–126. https://doi.org/10.1089/elj.2020.0633

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, *22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Husaini, M. R., Aliyatunnisa, N., Aini, N., Marliasari, R., & Rohman, Z. S. (2024). Peran Badan Pengawasan Pemilu dalam penanggulangan pelanggaran pemilihan umum di era digital dalam perspektif Undang-Undang Nomor 7 Tahun 2017 [The role of Bawaslu in addressing election violations in the digital era]. *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial dan Politik*, *1*(3), 153–169. https://doi.org/10.62383/demokrasi.v1i3.264

Karim, M. I. (2023). Strategi BAWASLU Provinsi Jawa Timur dalam mencegah pelanggaran pemilihan umum 2019 melalui media sosial [The strategy of Bawaslu East Java in preventing 2019 election violations through social media]. *Jurnal Politique*, *3*(1), 68–84. https://doi.org/10.15642/politique.2023.3.1.68-84

Kreiss, D., & McGregor, S. C. (2018). Technology firms shape political communication: The work of Microsoft, Facebook, Twitter, and Google with campaigns during the 2016 U.S. presidential cycle. *Political Communication*, *35*(2), 155–177. https://doi.org/10.1080/10584609.2017.1364814

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Sage.

Mozaffar, S., & Schedler, A. (2002). The comparative study of electoral governance: Introduction. *International Political Science Review*, *23*(1), 5–27. https://doi.org/10.1177/0192512102023001001

Norris, P. (2014). *Why electoral integrity matters*. Cambridge University Press. https://doi.org/10.1017/CBO9781107280861

Peraturan Badan Pengawas Pemilihan Umum Nomor 6 Tahun 2024 tentang Pengawasan Penyelenggaraan Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, serta Wali

Kota dan Wakil Wali Kota [Bawaslu Regulation No. 6 of 2024 on the supervision of regional head elections]. https://peraturan.go.id/files/peraturan-bawaslu-no-6-tahun-2024.pdf

Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital [Presidential Regulation No. 174 of 2024 on the Ministry of Communication and Digital Affairs]. https://peraturan.bpk.go.id/Details/306884

Prayoga, R. (2024, December 13). Bawaslu Jabar: Kebencian-hoaks Pilkada 2024 paling banyak di Tiktok [Bawaslu West Java: Hate speech and hoaxes in the 2024 regional elections mostly on TikTok]. *ANTARA Jawa Barat*. https://jabar.antaranews.com/berita/566185/bawaslu-jabar-kebencian-hoaks-pilkada-2024-paling-banyak-di-tiktok

Putri, L. U. M., Pebrianti, A., Elonika, Y., & Winarti, N. (2024). Aksesibilitas pengawasan media sosial oleh Badan Pengawas Pemilihan Umum terhadap pencegahan kampanye propaganda [Accessibility of social media supervision by Bawaslu in preventing propaganda campaigns]. *JIIP: Jurnal Ilmiah Ilmu Pemerintahan*, *9*(1), 40–57. https://doi.org/10.14710/jiip.v9i1.21741

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). (2022). *Official Journal of the European Union*, L 277. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Salusu, J. (1996). *Pengambilan keputusan stratejik untuk organisasi publik dan organisasi nonprofit* [Strategic decision making for public and non-profit organizations]. Grasindo.

Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *The International Journal of Press/Politics*, *25*(3), 517–537. https://doi.org/10.1177/1940161220918740

Undang-Undang Nomor 1 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2014 tentang Pemilihan Gubernur, Bupati, dan Walikota menjadi Undang-Undang [Law No. 1 of 2015 on the Election of Governors, Regents, and Mayors]. https://peraturan.bpk.go.id/Details/37341

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Law No. 1 of 2024, second amendment to the Electronic Information and Transactions Law].

Undang-Undang Nomor 6 Tahun 2020 tentang Perubahan Ketiga atas Undang-Undang Nomor 1 Tahun 2015 [Law No. 6 of 2020, third amendment to Law No. 1 of 2015].

Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum [Law No. 7 of 2017 on General Elections].

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development* (A/RES/70/1). United Nations General Assembly.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (Council of Europe Report DGI(2017)09). Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage.