DIGITAL PEACEBUILDING

2024 Issue 4

Bottom-Up Elections: Crowdsourcing ICTs for the Prevention of Fraud and Violence

Tzion M. Jones

Executive Summary

This policy brief explores the extent to which crowdsourcing and Information and Communication Technologies (ICTs) can inform strategies for deterring electoral fraud and related violence. Electoral fraud, when exposed, often incurs violence public response. Election monitoring can itself encourage the use of electoral violence in lieu of fraud, and thus monitors struggle to prevent violence. ICT-enabled crowdsourcing has the potential to enhance the efficiency of election monitoring, especially in developing democracies. Its utility is dependent on strong civil societies and high civic engagement. Data validity and the potential for ICT-enabled insurgency or lateral surveillance are also challenges, and the rise of artificial intelligence brings additional risks of manipulation. Recommendations include investing in civic engagement, expanding ICT infrastructure, and further research into secure crowdsourcing in the AI context. These strategies aim to enhance election integrity and empower citizens to safeguard their own democracies.

Introduction

We live in a time of growing concern over the integrity of global democracy. Many of the world's democratic countries enter critical elections this year, against the backdrop of rapidly evolving artificial intelligence. At the same time, social media has steadily established itself as a pillar of election dynamics over the past decade or so. This policy brief seeks to examine methods for maintaining citizen-centric avenues of vertical accountability through the use of information and communication technologies, with a particular focus on crowdsourcing.

What is Electoral Fraud?

Electoral fraud can broadly be defined as any conduct seeking to corrupt the tabulation of ballots, certification of results, registration of voters, or otherwise illegally manipulate the results of an election.[1] Scholars tend to qualify electoral fraud by both its intentional obscurity and its violation of standing electoral law in a given country.[2] The legal definition of electoral fraud is therefore subject to change with the evolution of legislation and technology. A legalistic framework is nonetheless important in understanding electoral fraud, and distinguishing legitimate instances from legal-yet-unfavorable conduct. Electoral fraud can take a variety of forms, and by some accounts includes the use of violence and coercion against voters.[3]Still others find it useful to classify manipulation by force, or electoral violence, as a separate phenomenon from traditional fraud.[4] In any case, electoral fraud and the pursuit thereof can bring about violence in a number of ways.

1 Alvarez, R. Michael, Hall, Thad E., and Hyde, Susan D., eds. "Election Fraud : Detecting and Deterring Electoral Manipulation." Blue Ridge Summit: Brookings Institution Press, 2008.

2 Lehoucq, Fabrice. "Electoral Fraud: Causes, Types, and Consequences." Annual Review of Political Science 6, no. 1 (February 6, 2003): 233–56. https://doi.org/10.1146/annurev.polisci.6.121901.085655.

3 ibid.

4 Dawn Brancati and Elizabeth M. Penn. 2023. "Stealing an Election: Violence or Fraud?" *Journal of Conflict Resolution*, 67(5): 858:892.

Tzion M. Jones. Brown University, A.B. International & Public Affairs, Computer Science '22 and MPA '24. | tzionmjones@gmail.com

Editor: Dawn Brancati

Following Fraud: Conditions for Violence

Protesting Perceived Manipulation:
Public perception of a fraudulent election may incur violent response by the citizenry, regardless of the accuracy of such perceptions. The simple belief that fraud has occurred is often a more reliable predictor of violence and unrest post-election. [5]

Voters are more likely to respond violently to electoral manipulation when they feel they have little agency or are control over the circumstances.[6] To secure their position, incumbent parties may also employ violence in handling public protest following a fraudulent victory.[7]

Stringent accountability measures institutional constraints can deter violent suppression of post-election protest by limiting the legitimate uses of force and introducing consequences for illegitimate uses.[8]

The Role of Election Monitors:
In a similar vein, the presence of external election monitors throughout can discourage candidates from fraudulent manipulation altogether.[9]

However, when electoral monitors expose and produce evidence of electoral fraud, the citizenry or political opposition may pursue collective action in the aftermath, including the use of force.[10] Additionally, once exposed, incumbents are not deterred from violence by the presence of observers as their corruption is no longer a secret. [11]

Further still, when election monitors are present, incumbents may actually pursue violent manipulation in favor of traditional fraud, as it is easier to tell whether their proxies and client networks have shirked their obligations.[12]

In sum, while monitoring elections can deter non-violent forms of fraud, they do not prevent violence on their own and in fact create new opportunities for it.

Monitors' capacity for violence prevention is limited by a number of other factors.

- *Conflicting Mandates:* Some scholars call for explicit violence prevention mandates for monitoring operations, citing their ability to mediate between opposing groups, coordinate with security forces, map out areas at increased risk for conflict and devise preemptive strategies. Others believe these additional responsibilities will detract from their primary goal of assessing election integrity. [13]

  In any case, proper violence prevention mandates typically require large and flexible budgets not reliably available to the organizations in question. [14]
- *Host Country Context:* Also of import are the sociopolitical conditions on the ground immediately prior to an election, and before the deployment of foreign monitoring operations. Developments concerning voter registration, delimitation of constituencies, and selection of party candidates in the host country are critical elements in the potential for violence that may take place before external monitors can collect the data.

  Scholars advise greater cooperation with local monitoring groups who may be privy to such information and can organize violence prevention efforts, but are less willing to openly criticize the validity of the election. [15]

Harmonizing deployments and systems of information with domestic actors and civil society organizations is promising, cost-effective way to improve violence prevention efforts in election monitoring.

As the next section will demonstrate, many of the shortcomings in violence prevention associated with election monitors can be alleviated with the help of

5 Daxecker, Ursula, Jessica Di Salvatore, and Andrea Ruggeri. "Fraud Is What People Make of It: Election Fraud, Perceived Fraud, and Protesting in Nigeria." *The Journal of Conflict Resolution* 63, no. 9 (2019): 2098–2127. https://www.jstor.org/stable/48597413.

6 ibid.

7 Hafner-Burton, Emilie M., Susan D. Hyde, and Ryan S. Jablonski. "When Do Governments Resort to Election Violence?" *British Journal of Political Science* 44, no. 1 (2014): 149–79. http://www.jstor.org/stable/43821581.

8 ibid.

9 Smidt, Hannah. "From a Perpetrator's Perspective: International Election Observers and Post-Electoral Violence." *Journal of Peace Research* 53, no. 2 (2016): 226–41. http://www.jstor.org/stable/43920011.

10 Daxecker, Ursula E. "The Cost of Exposing Cheating: International Election Monitoring, Fraud, and Post-Election Violence in Africa." *Journal of Peace Research* 49, no. 4 (2012): 503–16. http://www.jstor.org/stable/41721603.

11 Smidt, "From a Perpetrator's Perspective: International Election Observers and Post-Electoral Violence." 230-231.

12 Brancati & Penn, "Stealing an Election: Violence or Fraud?"

13 Garber, Larry. "Contemporary Election Observation Challenges." *Violence Prevention through Election Observation*. US Institute of Peace, 2020. http://www.jstor.org/stable/resrep26058.6.

14 ibid.

15 ibid.

Case Study: 'Photo-Quick Count' Monitoring and Aggregation Fraud in Afghanistan[1]

In many developing countries, democratic institutions are young and fragile, leaving electoral processes susceptible to corruption from networks of political elites. During Afghanistan's 2010 parliamentary election, Callen and Long used novel crowdsourced monitoring technology to detect fraudulent vote tabulation in favor of influential candidates.

The monitoring technique, dubbed 'Photo Quick Count,' involved taking on-site photographs of election returns forms (i.e. candidate vote tallies) at local polling centers immediately following election day, and comparing them to photographs of the same forms at provincial and national aggregation centers after the months-long tabulation process. In a clean election free of manipulation, the aggregate tallies for each candidate would be consistent throughout.

The experiment required photography and hand-coding of about 49,000 vote entries for 1,784 candidates at 471 polling stations across the country, made possible only by employing a decentralized citizen-based research team. Citizen researchers also wrote letters to a smaller sample of tabulation officials informing them of the crowd-based Photo Quick Count system and how it worked, which significantly reduced incidence of tampered, missing, or inconsistent data from respective centers. Crowdsourcing allowed the entire operation to be completed on a budget of $100,000 USD. For comparison, the largest monitoring operation by an entirely foreign team for the same election was only able to visit 85 polling stations.

The 'Photo Quick Count' experiment demonstrates a cost-effective, scalable, method of vertical accountability well-suited to crowdsourced implementation and viral adoption. It also requires very little international support, encouraging more engaged citizenship and strengthening democratic institutions. Callen and Long anticipate even lower costs and broader scope as the country's cellular networks and infrastructure expand.

1 Callen, Michael, and James D. Long. "Institutional Corruption and Election Fraud: Evidence from a Field Experiment in Afghanistan." The American Economic Review 105, no. 1 (2015): 354–81. http://www.jstor.org/stable/43497063.

ICT-enabled crowdsourcing techniques.

How Crowdsourcing Can Help Fill the Gap

In simplest terms, crowdsourcing is the mobilization of the general public, including online communities, for the completion of small tasks that incrementally contribute to a larger significant goal. Crowdsourcing, in conjunction with various ICTs, can address many of the limitations to violence prevention in traditional election monitoring.

Crowdsourcing is especially useful in the developing world where administrative capacity of democracies is low and the decentralized 'crowd' can accomplish tasks that usually require complex bureaucracy.[16]

Two recent case studies of elections in Afghanistan show that increased cell phone penetration and citizen-based monitoring ICTs can significantly reduce instances of electoral fraud. [17]

When novel monitoring technologies are introduced to clients of incumbents carrying out manipulation, fraud in favor of well-connected candidates is found to occur less frequently. Crowdsourcing can therefore allow election monitors to systematically deter key agents of corruption from carrying out fraud on candidates' behalf. [18]

In addition to deterring fraud, crowdsourcing can also prevent violence during and post election. The literature indicates two primary factors at play.

First, mobile phone networks allow citizens to laterally share information that organically neutralizes conflict. Second, crisis mapping software, SMS-to-radio broadcasts and other ICTs allow information aggregated from the crowd to quickly reach the ears

16 Livingston, Steven. "ICT's Role in Fighting Crime in Africa." Africa's Information Revolution: Implications for Crime, Policing, and Citizen Security. Africa Center for Strategic Studies, 2013. http://www.jstor.org/stable/resrep19165.5.

17 Gonzalez, Robert M. "Cell Phone Access and Election Fraud: Evidence from a Spatial Regression Discontinuity Design in Afghanistan." American Economic Journal: Applied Economics 13, no. 2 (2021): 1–51. https://www.jstor.org/stable/27087096.

18 Callen, Michael, and James D. Long. "Institutional Corruption and Election Fraud: Evidence from a Field Experiment in Afghanistan." The American Economic Review 105, no. 1 (2015): 354–81. http://www.jstor.org/stable/43497063.

of civil society leaders and larger organizations for timely response.[19]

Additionally, crowdsourcing can enable the collection of precise local data in real time. This effect can be further enhanced via ICT-enabled capacity building programs that teach citizens to identify critical risk factors and opportunities for response within their local context.[20] Locally crowdsourced information from an engaged civil society can therefore aid in the contextual adaptation of monitoring operations pre-deployment.

Early warning systems involve anticipating moments of escalation, collecting and relaying information about potential crises, assessing said information and developing a timely and appropriate response. In this context, early warnings can identify precursors to violence as well as corruption, as seen in the Afghanistan case with secondary vote tabulation.

A 2017 study of the Nigerian context found that ICT-enhanced early warning systems can be a powerful tool for stemming violent outbreak post-election in the Global South, but stressed the importance of corresponding frameworks for early response to such warnings.[21] These frameworks and their capacity will vary across contexts, but the literature highlights the critical role of civil society organizations in validating the use of crowdsourcing technologies.[22] Community-based prevention systems that funnel information on potential escalation or corruption to reputable social leaders trained in mediation can improve dynamic early response while strengthening cooperation between monitoring institutions and the electorate.[23]

Where conditions allow for effective early warning and response to electoral fraud and violence, and where individual agents of corruption can be identified and made aware of the monitoring technologies in place, those agents may not act on obligations to their incumbents for fear of being held accountable. In turn, the preference for client-based violent manipulation among externally monitored incumbents may be reduced.

Crowdsourcing and ICTs provide people-centric methods of deterring electoral fraud and violence while empowering the electorate to take ownership of their democracy. Humanist methods are especially critical in the context of rapid automation and artificial intelligence. Increasing local agency in violence prevention reduces reliance on elite-level response mechanisms, which in turn may reduce the likelihood of violent response when these elite-level mechanisms fail to protect election integrity.[24][25][26]

Crowdsourcing's Potential Pitfalls

Crowdsourcing is not without its shortcomings. A number of factors influence its potency in deterring both violence and fraud.

- *Civil Society and Civic Engagement:* ICT crowdsourcing efforts are only as good as their respective civil societies. [27] Strong civil societies can only make use of ICTs insofar as they are well-distributed across populations.[28] Further, increased ICT penetration or mobile phone ownership does not, in itself, imply increased civic engagement and vice versa.[29] The technology changes the nature of civic engagement and mobilization, but is not a substitute. Recent reports suggest social media can be strategically utilized to help cultivate civic engagement and strengthen the role of civil society.[30]

- *Data Validation:* Ensuring truth and validity of crowdsourced data without compromising response time is a major challenge. Organizers must consider the interests and biases of those re-

19 Martin-Shields, Charles, And Elizabeth Stones. "Smart Phones And Social Bonds: Communication Technology And Inter-Ethnic Cooperation In Kenya." Journal of Peacebuilding & Development 9, no. 3 (2014): 50–64. https://www.jstor.org/stable/48603499.

20 Alihodžić, Sead. "Electoral Violence Early Warning And Infrastructures For Peace." Journal of Peacebuilding & Development 7, no. 3 (2012): 54–69. https://www.jstor.org/stable/48603421.

21 Martinluther, Nwaneri, and Uwakwe Ikechukwu Stanley. "Harnessing Early Warning Systems as Instrument for Prevention of Post-Election Violence in Nigeria." Journal of African Foreign Affairs 4, no. 1/2 (2017): 163–79. https://www.jstor.org/stable/26664045.

22 ibid.

23 Alihodžić "Electoral Violence Early Warning And Infrastructures For Peace."

24 Martin-Shields & Stones, "Smart Phones And Social Bonds"

25 Tsuma, William, Christy McConnell, Peter Mwamachi, and Anne Kahl. "Crowdsourcing for Collaborative Prevention: Strengthening the 4th Generation Conflict Early Warning for Multi-Stakeholder Response." Peace Infrastructures, 2012. https://www.peaceinfrastructures.org/documents/crowdsourcing-collaborative-prevention.

26 Maina, Grace. "New Technology for Peace in Kenya." Edited by Andrea Ó Súilleabháin. Leveraging Local Knowledge for Peacebuilding and Statebuilding in Africa. International Peace Institute, 2015. http://www.jstor.org/stable/resrep09572.9.

27 Livingston, "ICT's Role in Fighting Crime in Africa"

28 ibid.

29 Martin-Shields & Stones, "Smart Phones And Social Bonds"

30 Dubow, Talitha, Axelle Devaux, and Catriona Manville. "Civic Engagement: How Can Digital Technology Encourage Greater Engagement in Civil Society?" RAND Corporation, 2017. http://www.jstor.org/stable/resrep17637.

Case Study: Crowdsourced Voter Surveillance and Coercive Campaigning in Israel[1]

In modern democratic societies, political campaigns increasingly employ digital tools to monitor and influence voter behavior. During Israel's March 2020 election, the Likud party used the Elector app, a sophisticated crowdsourced voter surveillance (CVS) tool, to mobilize supporters and track voter engagement. Anat Ben-David's 2023 study investigates the implications of such surveillance practices, revealing how they can transform ICT-enabled political participation into mechanisms of control.

The Elector app enabled party activists to monitor and influence voters by reporting their interactions in real time. The app collected extensive voter data, including personal information and political inclinations, allowing the party to target specific individuals with tailored messages and interventions. This approach, while enhancing voter engagement, raised significant ethical and privacy concerns.

Ben-David's research employed a mixed-methods approach, including digital ethnography of perceptions and usage of Elector, interviews with app developers, voters, and Likud campaigners, and an analysis of user data from the app to assess its scope and effectiveness mobilizing the electorate. The study found that CVS, enabled via Elector, turned citizens into active participants in lateral surveillance, compromising their own privacy and potentially undermining democratic principles. The app's widespread use illustrates how the same rhetoric of civic engagement and participation that are necessary to maximize crowdsourcing's positive impact can be leveraged by political candidates to control the outcome of an election, blurring the lines between legitimate political engagement and coercive manipulation.

The case of the Elector app in Israel's 2020 election highlights the dual nature of ICTs in the election space. While they can enhance voter engagement and facilitate bottom-up accountability frameworks, they also pose risks to privacy and democratic integrity in partisan hands. If crowdsourcing ICTs are to provide a citizen-centric approach to election integrity, the study underscores the need for robust regulatory and normative frameworks to ensure ethical usage that centers neutrality.

1 Ben-David, Anat. "Little Samaritan Brothers: Crowdsourcing Voter Surveillance" The Law & Ethics of Human Rights 17, no. 2 (2023): 127-165. https://doi.org/10.1515/lehr-2023-2008

porting in, and their impact on the data. Crowdsourcing also must rely on mixed-media submissions as different forms of communication are more accessible or trustworthy in different areas of a given state (e.g. urban blogs, rural newspapers).[31] Oversaturation of data, biased or not, can overwhelm and impede systemic response.[32] To mitigate this, aggregating submissions for verification by trained experts, before re-broadcasting from a single, trustworthy channel such as the radio or specialized monitoring platforms appears the most successful practice.[33][34]

- *Organized Violence:* Crowdsourcing and ICTs may also encourage organized violent responses to fraud, as they solve many collective action problems inherent to insurgency.[35] For example, private long distance communication enables greater in-group coherence and reduces certain free-rider problems.[36] Other research suggests this is a product of environments of decentralized, competing information without any collectively trusted sources. The information gaps create security dilemmas between ethnic or political groups that may incite violence.[37] This further underscores the value of rebroadcasting the voice of the crowd in aggregate, by external monitors with a claim to neutrality.

- *Automation and Social Control:* Much of the data collection for election monitoring described in this brief could be achieved nonconsensually via automation and social media scraping, especially with the rise of more powerful artificial intelligence. The bottom-up advantages of crowdsourcing are reversed in this scenario, and

31 Dowd, Caitriona, Justino, Patricia, Kishi, Roudabeh, & Marchais, Gauthier. "Comparing 'New' and 'Old' Media for Violence Monitoring and Crisis Response: Evidence from Kenya." Research & Politics 7, no. 3 (2020). https://doi.org/10.1177/2053168020937592

32 Mutahi, P. and Kimari, B. "The Impact of Social Media and Digital Technology on Electoral Violence in Kenya." Institute of Development Studies Working Paper 493, 2017.

33 Martin-Shields & Stones, "Smart Phones And Social Bonds"

34 Livingston, "ICT's Role in Fighting Crime in Africa"

35 Brennan, Glyn. "How Digital Media Reshapes Political Activism: Mass Protests, Social Mobilization, And Civic Engagement." Geopolitics, History, and International Relations 10, no. 2 (2018): 76–81. https://www.jstor.org/stable/26802343.

36 Pierskalla, Jan & Hollenbach, Florian. "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa." American Political Science Review 107 (2013). In Press. 10.1017/S0003055413000075.

37 Martin-Shields & Stones, "Smart Phones And Social Bonds"

the potential for exploitation, manipulation, and bypass of civil society are increased.[38] Grievance mechanisms for vulnerable populations may be an important application of ICTs as governments gain access to more powerful tools of manipulation. Again, the strength of ICTs is in their human connectivity.

Recommendations

Against the backdrop of rapidly evolving artificial intelligence technologies and increased potential for large scale state manipulation of democracy, it is important to safeguard and cultivate strategies for accountability and conflict prevention that center human beings. To that end, I recommend the following:

- Targeted investment in civic engagement and digital literacy programs, as well as expansion of ICT infrastructure in order to close digital divides, increase participation in crowd-reliant monitoring techniques, and maximize capacity for mobilization.

- Focus on harmonizing ICTs and crowdsourcing with extant election monitoring entities to expand their reach — this may include hiring local informants for contextual adaptations pre-deployment and designing early warning systems with trusted monitor organizations as a re-broadcasting point for collected data.

- Further research into the security concerns of anonymous crowdsourcing in the context of generative AI and human-like bots. Literature on AI, crowdsourcing ICTs and election monitoring is sparse now, but that may change following the influx of global elections in 2024. Research should be on the cusp of new developments so as not to act on obsolete conclusions.

38 Pauwels, Eleonore. "Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention: Opportunities and Challenges for the International Community." Global Center on Cooperative Security, 2020. http://www.jstor.org/stable/resrep27551.