Deficiencies in Electoral Security: Outcomes of the 2007 and 2013 Kenyan Elections

Citation

Permanent link
https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37365083

Terms of Use
This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA

Share Your Story
The Harvard community has made this article openly available. Please share how this access benefits you. Submit a story.

Accessibility

Matthew A. McKenna

A Thesis in the Field of Legal Studies
for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

May 2019
Abstract

Technology has forever changed the way we communicate. Whether sending an text message, transmitting email, or voting in a presidential election, technology has become a conduit for communicating our actions, choices, and intentions. In the context of a presidential election, technology plays a major role in key political outcomes. The violence in Kenya during its 2007 presidential election is a first-hand example where a lack of technology security caused a chain of events that scarred Kenyans for decades thereafter. An investigation into the voting technologies and election machines used during the election revealed catastrophic oversights by the Kenyan government. The ensuing investigation confirmed that no technology security had been put in place to verify and authenticate each voter’s identity for the election.

This thesis examines the political environment in Kenya, both prior to and following the 2007 election. It includes a discussion of how ethnic groups and voting sites contributed to the violence, displacement, and death of thousands of people during the timeframe surrounding the election. Investigation of Kenya’s Independent Electoral and Boundaries Commission was undertaken to determine whether key security aspects of the voting machines and processes were omitted by intent or unintentionally.

The analysis found evidence that technology security, including authentication practices to validate each voter, were neglected by the Electronic Vote Transmission systems used during the election. Further analysis was undertaken of the published
findings of the Kriegler Commission, which was formed to investigate the 2007 electoral operations, including irregularities leading to the election outcome.

As a comparison, the 2013 Kenyan election outcome is also analyzed, which found a positive direction taken by the Kenyan government, including reforms to the national constitution and the implementation and use of technology security for electoral voting machines as methods for reducing fraud. As a result, the 2013 elections were peaceful, reflected the underlying spirit of the election, and provide a very different outcome from the 2007 election. This improved state attests to the acknowledgement of and the need for strong measures to be taken by the Kenyan government to increase awareness, literacy, and effectiveness by securing critical technologies, beginning with the electoral machines.
Acknowledgements

I offer sincere gratitude to my thesis director, Professor John M. Mugane of Harvard University’s Department of African and African American Studies, for supporting and guiding each phase of this thesis project. I would also like to thank my research advisor, Professor Doug Bond, for all his effort and ongoing support.

Special thanks to my Mom, Dad, sister, my buddy Tommy aka Johnny, and my Maddy for supporting me throughout all my academic pursuits. Much of my inspiration has been fueled by your good wishes, guidance, and unwavering support, for which I am forever grateful.
Table of Contents

Acknowledgements........................................................................................................... v
List of Tables and Figures...............................................................................................vii
Glossary of Acronyms ...................................................................................................viii
Chapter I  Introduction ............................................................................................... 1
Chapter II  2007: Before the Election ................................................................. 3
Electronic Voting Transmission ............................................................... 4
Ethnic Groups, Voting, and Violence ....................................................... 7
Deploying Electoral Machines .................................................................. 9
Biometric Voter Registration.................................................................. 12
Electronic Voter Identification System................................................... 13
Risks........................................................................................................ 14
Chapter III  2007: Post-Election Implementation and Impacts .................... 15
The Kriegler Commission ........................................................................... 15
Vote Counting and Tallying................................................................. 16
IREC Findings ........................................................................................ 17
Recommendations .................................................................................. 17
Independent Electoral and Boundaries Commission .............................. 18
Chapter IV  2013 Election: Scenarios and Outcomes ................................................. 20
Chapter V  Conclusion .............................................................................................. 24
References ....................................................................................................................... 26
List of Tables and Figures

Table 1  Candidate Performance.................................................................................. 6

Figure 1. Gallop Poll, Kenyan Election 2007 ............................................................... 8
Glossary of Acronyms

BVR  Biometric Voter Registration
ECK  Election Commission of Kenya
EVID Electronic Voter Identification Device
EVIS  Electronic Voter Identification System
EVT  Electronic Vote Transmission
ICT  Information Communication and Technology
IEBC  Independent Electoral and Boundaries Commission
IREC  Independent Review Commission
Chapter I

Introduction

From 1963 to 1990 Kenya had a monolithic, one-party system of government that could be characterized as presidential authoritarianism. During this time, Kenya resisted most of the Marxist-Leninist ideologies that swept through Africa during the 1960s and 1970s, although the national political environment was marred by civil strife and violence. In the early 1990s, Kenya reached a major political landmark by reforming its constitution and permitting the first multi-party election since the country achieved independence. This milestone widened the door for political diversity and defined how the government would approach the electoral process in coming years (Ndungu, 2008).

As Kenya expanded economically, it also began to focus on technologies that could harness and tally voter information during elections. It is important to keep in mind that throughout the 2002 election period, the country continued to shed its authoritarianism roots and began to emerge from cultural silence. At the same time, its political system remained sharply divided by issues including land allocation, religion, literacy, and multiple ethnic groups—all of which contributed to instances of periodic extreme violence.

However, Kenya, like many other countries, began to embrace the use of new technologies to strengthen its social and political posture. It was not unreasonable that expertise that dealt specifically with cyber security and the protection of software and infrastructure technologies would be limited in the beginning. As a result, strategies for
how to develop and deploy security programs that focused on securing software applications as measured by policy and governance tracking were not top of mind.

Rather, getting the technology into use was the primary goal, which Kenya successfully achieved. The benefits of enabling a systematic process that reduced manual workflows for elections was a step in the right direction, enabling Kenya to better position itself for future advances and leverage cutting-edge technologies to become stronger as a country.

This led to the use of multiple devices aimed at providing a cohesive solution to a central problem for Kenya: establishing a system of records that could validate voter identity and provide a platform for registering to vote and casting ballots. Several key technologies were deployed to achieve this outcome. The backdrop leading up to the 2007 presidential election period is what I refer to as the Before Scenario and it is here that the use of electoral machines begins.
On December 30, 2007, Mwai Kibaki began his second term as Kenya’s third president, but this time it felt quite different from his first swearing-in ceremony in 2002, standing in front of approximately one million citizens in Nairobi’s Uhuru Park. This time his inauguration was held inside his official office residence in the State House. The audience was small by presidential standards, with only the state broadcaster present (Cheeseman, 2008). At the heart of that inauguration, however, was electoral malpractice alleged by national and international observers who believed that the results were flawed, possibly even even rigged. As a result, fingers were pointed at people, processes, and underlying technologies in use during the 2007 election.

At the time, Kenya was plagued by violence, some of which was believed to stem from the improper use of technology, which in turn produced certain outcomes from the election. At the center of this turmoil was the newly deployed Electronic Voting Transmission (EVT) technology. Unlike manual voting systems used in prior elections, EVT was meant to relay results quickly and efficiently to avoid long waiting periods between voting and releasing results (Halakhe, 2013). It was further hoped that accuracy would be sharper with the reduction of manual and error-prone legacy processes such as those used prior to the deployment of electoral machines and other mobile technology devices. However, such technology still did not remove either the possibility of human error or the susceptibility of results being negatively impacted or compromised by
hackers and cyber attacks. Hovering over everything was a lack of expertise and knowledge about how to track, monitor, and protect data. Later, it became evident that no prior security testing or penetration testing was conducted in an effort to identify potential weaknesses or vulnerabilities in the software running the electoral machines.

Electronic Voting Transmission

The Electronic Voting Transmission (EVT) system relies on mobile devices used by a presiding officer or administrator to enter election voting data from each collected voter form into a specially developed mobile phone application. According to the Independent Electoral and Boundaries Commission (IEBC), the software and physical device together are presumed to securely transmit data over a mobile data network to the IEBC headquarters for tabulating and publicizing (Halakhe, 2013).

It was intended that data from the EVT system would flow from each regional polling station to the main counting center, and then to the end destination located in Nairobi. As with any new technology, it is not uncommon to experience outages or latency issues that may affect results to and from destination points. While such issues can stem from a variety of underlying causes not necessarily related to security, it became apparent that the EVT system had not undergone any form of stress testing before it was deployed regionally. On voting day, it was reported that multiple system failures occurred. Preliminary information collected by the IEBC investigation suggested that system password failures played a minor but pivotal role in the decision to discontinue using the system and to revert to a manual vote tallying process rather than trust the EVT results (Halakhe, 2013).
In February 2008, the Kenyan government established the Independent Review Commission (IREC) to investigate the technology and determine whether there was any indication of malice or intentional manipulation. During the investigation, the Election Commission of Kenya (ECK) was questioned, as they were responsible for the overall architecture and management of key components of voter registration on election day.

It is important to note that there had been a history of confidence in the mechanics and certification process because it had performed well in the 2002 and 2005 elections; it was believed to be credible and capable of securely managing and transmitting voter data. However, the general confidence and integrity of the ECK abruptly changed when President Kibaki made a last-minute political decision to appoint 18 new commissioners among 21 total positions. Those newly hired commissioners lacked expertise and technical aptitude to carry out several of the technical security improvements recommended by the previous Commission (Leonard & Owuor, 2007).

Ostensibly, Kibaki’s decision could be interpreted as highly coincidental given the events that unfolded following the election. It further begs the question: why did former members of the ECK not raise a red flag with local government affiliates? Why were proper training and technology literacy overlooked? In hindsight, it could be argued that Kibaki’s decision indicated that he was reasonably aware of the technology’s limitations and that by removing those with some degree of technical knowledge, there remained new commissioners with less knowledge – a convenient scapegoat when the time came to identify technical vulnerabilities. In essence, no one could fix the problem because the problem was not technically understood. The ensuing unreliability of the
people, process, and technology, as demonstrated by the faulty tabulation process, would reduce public trust in the Commission.

On the evening of March 5, 2008, the Commission acknowledged that a failure had occurred in the electronic transmission system. The IEBC immediately summoned some 290 election directors to Nairobi to manually tabulate ballots and confirm election results (Thibon, et al., 2015). At the end of the investigation, and based on data collected and analyzed by the Commission, the results revealed an unlikely (to some) outcome (see Table 1).

Table 1. Candidate Performance.

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Coalition/Party</th>
<th>Votes</th>
<th>% Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mwai Kibaki</td>
<td>Party of National Unity (PNU)</td>
<td>4,584,721</td>
<td>46.42</td>
</tr>
<tr>
<td>Raila Odinga</td>
<td>Orange Democratic Movement (ODM)</td>
<td>4,352,993</td>
<td>44.07</td>
</tr>
<tr>
<td>Kalonzo Musyoka</td>
<td>Orange Democratic Movement - Kenya (ODM-K)</td>
<td>879,903</td>
<td>8.91</td>
</tr>
<tr>
<td>Joseph Karani</td>
<td>Kenya Patriotic Trust Party (KPTP)</td>
<td>21,171</td>
<td>0.21</td>
</tr>
<tr>
<td>Pius Muiru</td>
<td>Kenya People's Party (KPP)</td>
<td>9,667</td>
<td>0.1</td>
</tr>
<tr>
<td>Nazlin Omar</td>
<td>Workers Congress Party of Kenya</td>
<td>8,624</td>
<td>0.09</td>
</tr>
<tr>
<td>Kenneth Matiba</td>
<td>Saba Saba Asili</td>
<td>8,046</td>
<td>0.08</td>
</tr>
<tr>
<td>David Waweru Ngethe</td>
<td>Chama Cha Uma (CCU)</td>
<td>5,976</td>
<td>0.06</td>
</tr>
<tr>
<td>Nixon Kukubo</td>
<td>Republican Party of Kenya (RPK)</td>
<td>5,927</td>
<td>0.06</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>98,770,288</td>
<td>100</td>
</tr>
</tbody>
</table>


During its investigation, the IREC released this statement: “The recorded and reported results are so inaccurate as to render any reasonably accurate, reliable, and convincing conclusion is impossible to ascertain” (Rheault & Tortora, 2008). Naturally (and perhaps rightfully so), attitudes regarding the honesty of the election process began
to crumble as trust and confidence diminished among the many voter groups. This led to a further loss of confidence in the credibility and reliability of the electoral machines.

Ethnic Groups, Voting, and Violence

The largest voter representation is ethnic groups, many of which reported a decline in confidence in the electoral process altogether. Results collected from a 2008 Gallup poll showed that fewer than 10% of Kamba, Luo, and Luhya groups, and 16% of Kalenjin had confidence in the election results (Rheault & Tortora, 2008). A subsequent poll, taken between June and July 2008, reported that an estimated 70% of Kenyans believed the election results were dishonest (Rheault & Tortora, 2008).

Many politicians in Kenya believe the route to power is through ethnic allegiance. For example, in 2007:

- Raila Odinga’s ODM Party was mainly supported by his Luo community and its neighbors the Luhya and Kalenjins, among others.
- Kenya’s largest group, the Kikuyu, broadly supported the PNU Party and Kikuyu President Mwai Kibaki;
- Kalonzo Musyoka’s ODM-Kenya was largely backed by his Kamba people south and east of Nairobi.

Five of the most prominent ethnic groups—Kamba, Kalenjin, Kikuyu, Luhya, and Luo—participated in opinion polls to determine how ethnic attitudes affected the election outcome in 2007. According to that poll (and shown in Figure 1), the top five groups, representing approximately two-thirds of the national population (Kikuyu 19%, Kalenjin 15%, Luo 13%, Luhya 12%, and Kamba 9%), believed the election results were
dishonest and inaccurate. Soon after the elections, there was a general revolution against the government and among the people.

Figure 1. 2007 Election Results, Gallup Poll.


That 2007 election period witnessed the highest number of opinion polls ever conducted in Kenya, and as a result the manipulation of opinion and electoral results became apparent to everyone. The use of the public opinion polls provided valuable insight on the reactions of the population, and induced important and often intense discussion and debate on key issues. It is clear that opinion polling plays a significant role in how Kenyans participate and share their political choices, adding further credence to the need for trained experts to manage the electoral machines.

After the election results were publicized, and the ECK announced Kibaki’s defeat of Raila Odinga (the main opposition leader representing the Orange Democratic
Movement) (ODM), ODM supporters accused the Kibaki’s PNU party of rigging the polls and then staged street protests, resulting in violent ethnic attacks, especially in the densely populated and mixed Rift Valley regions (BBC, 2013). While reports varied regarding the total number of casualties, it is believed that between 800 and 1,500 deaths occurred, and 100,000 to 300,000 people were ultimately displaced (Cheeseman, 2008). The violence resulted in social fragmentation among the ethnic groups in areas hardest hit by the violence.

This scenario illustrates the role of technology, even beyond presidential elections. The ability of technology to unite or divide people is more powerful, perhaps, than the idea of democracy itself. Consequently, in the next chapter I take a deeper look into how the electoral machines were selected, and the impact they have following deployment.

Deploying Electoral Machines

As technology advances, mobile devices, tablets, and other electronics are becoming common in modernized communication. While there are many advantages with these devices, there are also information security risks to be considered. During the 2007 Kenya election, a lack of formal policies and risk governance procedures for securing critical government and business systems was the proximate cause of political mayhem and outsize influence on the outcome of that election.

Examining the social and political impacts of technology plays an important role in how government actors confront security breaches, cyber attacks, and data manipulation. As Kenya continues to develop and deploy information communication
and technology infrastructures (ICT), the government must enhance legal and policy mandates around securing software and critical business systems—specifically the software applications that collect and analyze voter information from electoral voting machines. As dependence on these technologies deepens, the focus must turn to ensuring an appropriate level of security that will create and scale a fair political system (Okuku, 2015).

As an example, among mobile devices the applications that are downloaded by end users are typically overlooked. Given the convenience and diversity of access points, it is not surprise that mobile applications have introduced a level of risk that most consumers are simply unaware of. It is fair to say applications were not always developed with security in mind. Rather, most applications provide users with access to specific points of interest or information. Mobile banking, email, calendars, weather, are among a variety of commonly used applications. In the same way, state and government agencies have increased their use of mobile devices – and have tied the country’s democratic electoral process to the use of electoral voting machines. Many other countries rely on a variety of technologies, while knowledge about the use and security of these devices have not kept pace with their increased level of use and sophistication. As a result, more attacks, data leaks, and manipulation have caused a severe threat to the population, the government, and to democracy itself.

Accordingly, this research aims to further understand how the Kenyan government is confronting these threats to their election system through the use of these electoral machines. Considerable attention was given to understanding and assessing
steps Kenya might take to solve these problems and apply lessons learned even as the country increasingly depends on leveraging multiple technologies.

To acquire first-hand information that would enable me to put this thesis into proper context, I examined several electoral machines from the viewpoint of each question posed below. This put each of the electoral machines under scrutiny, and level-set the outcomes leading to and after the 2007 election.

1. What training was provided either by the Kenyan government or the manufacturer of the technology prior to implementation and regional deployment?

2. What level of security testing was done prior to implementation and deployment?

3. Were any preventive measures taken to ensure that the software was encrypted prior to securely transmitting data?

Determining a clear response and approach to deploying these technologies is critical to producing positive political outcomes in the future. However, without clarity and a plan in place, Kenya will continue to find itself repeating history. Additionally, as mobile devices continue to have a major role in how people interact and engage with one other and the government, it is reasonable to believe that attacks will increase in frequency and severity.

From a legal perspective, Kenya must elevate its prosecution of attackers or those who are willfully blind to the need for a responsible level of security to help reduce future behaviors. During the 2007 election period, many went unprosecuted for their crimes or negligence (ENISA, 2013). A full examination of the security decisions made by the
Kenyan government to protect itself from malpractice and attacks, as well as looking into IEBC and IREC, will provide insight into the ongoing strategies and approaches being considered. Ultimately these agencies should help increase visibility into the critical need for Kenya to protect its democracy by securing technology and increasing literacy for those in positions to handle electoral machines and manage election processes.

Biometric Voter Registration

Biometric Voter Registration (BVR) works in tandem with Electronic Voter Identification Devices (EVIDs) to identify voters. Biometric technology uses cameras, laptops, and fingerprint scanners to capture fingerprints, facial biometrics, and other information (such as name, sex, age, ward, county) to authenticate a voter’s identity. The use and implementation of any new technology brings with it a degree of risk. Although not a constitutional requirement, BVR could be implemented to enhance the integrity of the voting process. This use of the technology would provide a well-structured program for collecting and authenticating voters while also establishing a central repository for tabulating results.

From a training perspective, teams would need to undergo a period of professional training leading to the large-scale deployment of BVR systems. But without adequate training, errors occur as was amply demonstrated by many stations that encountered problems while using BVRs during the 2007 election. According to newly developed best practices for deploying BVRs, a governance framework that works in conjunction with security practices already in place is critical to ensure a timely response in the event of mechanical breakdowns (ENISA, 2013). This leads directly to accurate
results by creating authentication access points for users, which is key to providing protection against attacks and ensuring that the privacy of voter data is maintained. These key factors were not applied when electoral machines were used in the 2007 election.

Electronic Voter Identification System

The Electronic Voter Identification System (EVIS) is an electronic poll management system that has two underlying technology components: a laptop, and an attached fingerprint reader connected directly to the laptop. An EVIS verifies voters electronically by communicating with BVRs. They check in each voter at a polling station, which streamlines the voters’ experience by reducing processing and wait times. From a risk perspective, EVIS ensures that only those who are registered and have a valid known identity as recorded by BVR are eligible to vote (IEBC, 2018). From a training standpoint, this device is quite intuitive and not overly complex to use, although basic technical literacy is needed. So training is not as critical for the first component of EVIS.

The second process, which has an optical technology component, is also relatively intuitive. From a security perspective, however, handling the data is most critical, and proved to be the central point overlooked during the 2007 election. Given that the device communicates with BVRs, a certain level of encryption was needed to ensure the data was accurate and not altered. It is important to note that while there were no specific allegations regarding EVIS, it would be reasonable to assume that if information had been duplicated during the process of transmission—which was a known vulnerability for BVRs at the time—the results could have been compromised and reported inaccurately (ENISA, 2013).
Risks

Risk is associated with the use of any technology, and the electoral machines were not exempt. To mitigate this risk, a formal repository of voter records as well as a citizen identity system must be in place to authenticate every voter. If a country cannot identify its citizens by a social security card or birth certificate, it becomes problematic when a solution is proposed that requires validation of each voter and which vote corresponds to each person. In the case of the 2007 election, the data was not properly organized, which required manual reviews. Such a manual system can lead to a person casting multiple votes—a problem that occurred in Kenya in both the 2007 and 2013 elections. Authenticating each voter and his/her personal identity information is critical to the value provided by ICT and the electoral machines themselves.
The Election Commission of Kenya (ECK) is empowered under the National Assembly and Presidential Elections Act to bring appropriate sanctions or legal actions against any person(s) or group(s) associated with manipulating or tampering with election results (Leonard & Owuor, 2009). The ECK, in many instances, has been a sounding board of reason for Kenya, supplying Kenyan officials with recommendations on how to effectively strengthen Kenya’s constitution and legal frameworks as they relate to the use and implementation of electoral technologies.

The Kriegler Commission

In March 2008, the Independent Review Commission (IREC) was appointed by President Kibaki to investigate the 2007 election, including the people, processes, and technology used under the ECK’s administration. Informally referred to as the Kriegler Commission, it was comprised of members from both the PNU and ODM parties, and was charged with uncovering answers from a variety of perspectives.

Three main areas of the Kriegler Report were analyzed to assess their criticality and relevance. First, I explored the scope of the investigation including the role of the ECK, vote-counting, and the tabulation processes used. Second, I examined key findings of the Kriegler Report with specific attention on the validity and integrity of the results. Third, I make recommendations for future electoral processes, including best practices.
for implementing voter machine technologies and proposed legal recommendations for securing future elections.

Vote Counting and Tallying

To the detriment of Kenyans in general and specifically the 2007 elections, legislation that would have protected the integrity of the voting process was overlooked despite recommendations from the ECK, including specific advice regarding operations and tallying. At first glance, counting and tallying should have been a straightforward process. The process began at the constituency tallying center, where an officer collected material from the polling stations, verified that all requisite materials were present, and then submitted the materials to a presiding officer who oversaw the process of entering the information into a dedicated management system.

Next, all polling stations in the constituency were required to render results by adding up columns archived in the BVR and EVID systems. Once this was completed, the results could simply be announced verbally, following the issuance of a Certificate of Results for both parliamentary and civic election winners (Kriegler and Waki Reports, 2009). According to the IREC, the results were delivered by telephone immediately after each constituency tallying was completed, which was the primary source of confusion at the national tallying center (Kriegler and Waki Reports, 2009).

Not surprisingly, as with many manual processes, the probability for error increased. The investigation found that a key reason behind the 2007 election outcome was the failure to establish a process capable of authenticating each voter. This was a
critical step overlooked in the 2007 election, but it would emerge again in the 2013 elections as processes and best practices for electoral machines were instituted.

IREC Findings

The IREC report highlighted important aspects of the Commission’s finding, including analysis of the testimony of witnesses who gave depositions and recorded statements between July and September 2008 (Kriegler and Waki Reports, 2009). The key takeaways were:

- Approximately 1,133 people died as a result of post-election violence, with the highest number of deaths (744) concentrated in the province of Rift Valley.
- Approximately 3,561 people reported injuries from blunt objects.
- A total of 117,216 private properties, houses, and commercial premises were destroyed, including 491 government-owned facilities.
- Approximately 350,000 people were displaced from their residences and/or business.

This information supports the finding that if proper attention had been given to utilizing security and risk technologies to protect electoral machines and prevent manipulation, the election outcome could have been quite different.

Recommendations

The IREC urged that a refinement be made to Kenya’s constitution that would provide guidance on the electoral process, including legislation added to the existing National Assembly and Presidential Elections Act as sections 3-3B (Kriegler and Waki
Reports, 2009). This turned out to be an important recommendation. Much of the 2007 election crisis stemmed not just from a lack of process (including the role of electoral machines), but also how officials handling vote data were trained, and how discrepancies in the data would be reviewed. The result was that the approach taken was not effective at governing results and producing positive outcomes that reflected accurate voter sentiment.

To achieve the desired outcome, the IREC recommended basic training, such as Building Resources in Democracy Governance and Elections (BRIDGE, 1999). The IREC further advocated the importance of recruiting election personnel that were properly vetted to reduce fraud in the handling of voter data (Kriegler and Waki Reports, 2009).

The Independent Electoral and Boundaries Commission

The IEBC was initially established to conduct and supervise elections and referenda in Kenya. Its core functions as they pertain to the voting process included: continuous registration of citizens as voters; delimitation of constituencies and wards; regulation of the process by which parties nominate candidates for elections; settlement of electoral disputes, including those related to nominations; and voter education and facilitation of observation, monitoring and evaluation of elections (ELOG, 2013).

Several key factors fueled suspicion and mistrust of the IEBC following the 2007 election: flawed use of technology; failure to continuously register voters; unconvincing implementation of delimitation of boundaries to enforce proper training and use of technology in the electoral tabulation process; and inadequate enforcement of procedures.
and legal requirements for tabulating results. In addition, the IEBC failed to hold political parties accountable for some of the breaches that occurred in 2007 as it pertained to the Elections Act. Accordingly, Kenyans lost confidence in the IEBC because of these shortcomings, and demanded that future electoral processes become clear and transparent (ELOG, 2013).
Chapter IV

The 2013 Election: Scenarios and Outcomes

The shadow of the post-election violence in 2007, lingered over the next major
election, which was held on March 4, 2013. This was a presidential election which saw
Uhuru Kenyatta of The National Alliance (TNA) defeat Raila Odinga of the Orange
Democratic Movement (ODM).

On the plus side, more than 12 million Kenyans cast a vote (Ferree, Gibson &
Long, 2014)—the largest number of votes in the country’s history. This was also the first
election held under the auspices of a newly created constitution with changes that sought
to produce a more mature election process, including:

- how political parties and coalitions were registered and managed,
- defining the role and responsibilities of state bodies and institutions, including the
  IEBC,
- determining how election disputes would be mediated by the Kenyan judiciary in
  the event results were contested, and
- monitoring the role and use of electoral machines as a government agent for
  protecting election voting from fraud.

This revamped system empowered and expanded local and regional
administrators and their authority to oversee the election process. Despite many legal
loopholes that had to be resolved, for the 2013 election Kenya demonstrated a new and
improved path for conducting its elections and leveraging BVR and EVID technology.
Although voter registration proceeded relatively smoothly on election day, problems did emerge, including the failure of verification kits, and faulty mobile phone transmission of results to a dedicated server system. Additionally, polling station administrators reported problems with the EVID system used to identify voters and capture fingerprints, which failed to work in more than half of the polling stations.

Speculation about the validity of the election results emerged, with allegations of rigging made by candidate Raila Odinga, who ultimately rejected outright the results of the election and petitioned the Supreme Court directly. Later the Court struck down the Odinga case, although the effectiveness of the technologies remained in question.

The 2013 elections, like the 2007, contained a high degree of ethnicity-driven sentiment which played a key role in voting styles and candidate preferences. According to Ferree, Gibson and Long (2014), Odinga garnered more support on issues related to the implementation of 2010 constitutional reforms, while also drawing attention to issues of government corruption, violence, and the use of the International Criminal Court. Odinga drew on the 2007 violence as a way to project a need to improve security during and after elections.

On the other hand, candidate Uhuru Kenyatta championed the issues of economy, employment rate, and government security, especially around protecting voters at the polls. Kenyatta approached the issue of post-election violence by leveraging ethnic diversities, a well-known style that uses the affinity between co-ethnic citizens and candidates to establish and strengthen voter motivation (Ferree, Gibson, & Long, 2014). Given the highly diverse ethnic landscape of Kenya’s population, the formation of multi-ethnic coalitions played a pivotal role in Kenyatta’s success in winning the presidency.
Another important aspect of the 2013 election was full implementation of BVR and EVID technologies. Unlike the 2007 election when these technologies were being newly tested, full-scale deployment in 2013 made use of best practices and implementation strategies, including advanced training for operators and ongoing security testing of each electoral machine (Ferree, Gibson, & Long, 2014). In an effort to bring young voters to the polls, new communication tools such as social media and mobile devices helped both Odinga and Kenyatta to reach new audiences. Furthermore, it brought modernity to the political landscape, creating social platforms that enabled both candidates and the people to voice their opinions and share views. Best of all, it was a secure and safer platform for discussing differences of opinion and contentious issues.

Another positive outcome was greatly increased knowledge of the newly deployed voting machines, along with a plan to support them going forward, and not just during elections.

It is apparent from the positive outcomes of the 2013 election, that the use of information communication devices provided voters with easy and effective ways to cast their votes. Electoral machines improved the data collection process, tightened security to reduce data manipulation, and provided greater education and improved literacy. Using technology as a lens from which to analyze the 2007 elections provided valuable insights into how enhanced electoral technologies and improved processes utilized in 2013 were able to streamline the election process and reduce social friction.

The scenario after the 2013 election reveals an improved state. In terms of violence, Kenya experienced much less social uproar following the election. Additionally, Kenya implemented improved systems and matured processes to help
further the use of technology, thereby paving the way for new opportunities and improvements through the use of electoral machines.
Chapter V

Conclusion

Digital technology provides a variety of benefits to society, and the election process is no exception. When applied and used effectively, electoral technologies can provide benefits to many stages of the electoral cycle, from registering voters to counting ballots. For low-income countries, putting these new technologies to use can have a large impact. For decades, many countries relied on manual and paper-based processes that if not tracked and monitored, created opportunities for fraud. Paradoxically, harnessing these advancements (as has been done in numerous African countries over the past decade) continues to play a pivotal role in reducing errors, eliminating fraud, and helping to establish a fair and transparent election process.

Kenya is an excellent example of demonstrating before-and-after scenarios on the effects of implementing electoral technologies as a means of combating fraud and authenticating voters. The positive impact of well-constructed security programs, implementation strategies, and ongoing training and education will be critical to Kenya’s future. As I have shown, Kenya has made significant improvements over the past several decades. It is reasonable to expect that progress in the use of technology and securing critical business systems will increase visibility with government and its supporting agencies. Further, as global dependence on information and communication technologies continues, and the use of electoral machines remain the main vector of voting, literacy on these technologies will likely increase, thereby closing the gap even further.
The lessons and outcomes learned by exploring the sharp contrasts of where and how technology has influenced political outcomes is no clearer than in the case of Kenya. With continued research, other countries intending to use and implement electoral machines will learn and apply the scenarios and knowledge acquired by Kenya to prevent negative impacts. While much work lies ahead, the positive aspects of technology have created a sense of cohesion among people, processes, and technologies in the political and social spheres. As each area matures it is my hope that peace remains front and center, and that security will to evolve at a pace that continues to reduce deficiencies in electoral voting processes.
References

Works Cited


**Works Consulted**


