



Cyber security in enhancing democracy in Kenya

Dorcus Phanice Olasya^{1*}

Anita Kiamba²

Peter Kagwanja³

^{1*}dolasya@students.uonbi.ac.ke

¹<https://orcid.org/0009-0006-2365-7920>

²<https://orcid.org/0009-0008-3474-3861>

^{1,2,3}The University of Nairobi, Kenya

Recommended Reference: Olasya, D. P., Kiamba, A., & Kagwanja, P. (2025). Cyber security in enhancing democracy in Kenya. *African Quarterly Social Science Review*, 2(3), 216–226. <https://doi.org/10.51867/AQSSR.2.3.19>

Submitted: 17th July 2025; Accepted: 8th August 2025; Published: 25th August 2025

ABSTRACT

On 9th August, right after the 2017 General Elections in Kenya, the opposition leader, under the opposition party National Super Alliance (NASA), alleged that the Independent Electoral and Boundaries Commission's (IEBC) database had been hacked. The hack supposedly created an algorithm where an 11% gap was created in favor of the incumbent President. To support the claims, the opposition presented a log file giving an account of how and when the IEBC database was hacked into. What followed was a court petition whose ruling nullified the Presidential elections, calling for a rerun. Fast forward, in August 2022, the Azimio la Umoja One Kenya Alliance once again challenged the IEBC final presidential results, claiming inconsistencies in voter turnout as captured in the Kenya Integrated Election Management System (KIEMS) kits and Form 34C. Equally, reports emerged of an Israeli disinformation specialist, hired by unknown individuals, infiltrating Gmail and Telegram accounts of one of Kenya's presidential candidate's close political advisors. These, among other instances, represent some of the challenges Kenya is facing with the widespread adoption of technology into the different societal aspects. In the electoral process, technology was meant to enhance transparency and accountability to a process previously tainted by massive voter theft and result manipulation. However, with the new technological developments, new challenges have emerged. Further, with the penetration of the internet and social media adoption, new forms of manipulation have been encountered. Using the agenda setting theory, this paper demonstrates how novel technologies have influenced the Kenyan electoral process. Focusing on misinformation, fake news, among other issues, the study highlights the implications of these forms of manipulation during the past general elections. The findings indicate that although technology was to bring forth solutions to enhance democracy, it has not only turned out to be a source of dispute to the process, but also elicited the impression of destabilizing the process of participatory democracy. To mitigate against future interferences, a multifaceted approach with the involvement of all key stakeholders is proposed. The study adopts a qualitative and analytical research design with secondary data gathered from existing records, journals, and reports.

Keywords: Cyber, Data, Democracy, Elections, Technology

I. INTRODUCTION

The development of the internet signified a new era not only socially, but also in the democratic discourse encouraging open discussions while devolving power (Kornbluh et al., 2020). Its nature further toned down its entry barriers enhancing communication, sharing of content to audience globally while having access to a wide range of information. With this, the internet allowed the creation of new communities across geographical divide, at the same time enhancing the creation of nouvelle innovations. Through internet enabled technologies, prompt global communication can be achieved at no cost. Further, transparency has been heightened by pointing out power abuse, corruption and sloppiness within governments (Brooke, 2016). This has therefore opened up the government to citizens consequently strengthening democracy (Brooke, 2016). By providing a safe platform for the populace to speak out, democratization has been achieved creating new opportunities for interaction between representatives and represented as well as political and societal actors. Consequently, in the words of Berg et al. (2022) digitization has transformed the political arena; it has changed how political decisions are made.

During its inception, the internet offered a perfect environment for everyone to be seen and heard. This was made possible through its de-centralized and easily accessible infrastructure, that facilitated an easy flow of information, thus enhancing equality as well as fairness (Ezrachi & Robertson, 2024). The emergence of social networking sites also gave rise to free and real time access to information. With this, new methods of communication between politicians and



the electorates were developed hence shifting how voters are influenced (Gopaldas, 2019). Through the digital space and unlimited flow of information, citizens have been granted a chance of making independent democratic choices (Ezrahi & Robertson, 2024) promoting a citizen-centered governance. Accordingly, debates have emerged on the role of the cyber space and its effects to democracy within states.

In his view, Gopaldas (2019) notes that the internet has indeed facilitated the disruption of democracies. This is evidenced by a report by the Freedom House reporting a decline in global freedom for 18 consecutive years as at 2023 (Gorokhovskaia & Grothe, 2024). Additionally, the report highlights a decline in global freedom in 52 countries between the year 2022 and 2023, largely attributed to election manipulation which emerged as the principal cause of global erosion in freedom. And as the dependence of the citizens to mass media for information and opinion declines, possibilities of collective action, organized from anywhere across the globe increase (Berg et al., 2022) as was the case with the Arab Spring (Gopaldas, 2019). To Bailard (2014) however, the effects of the digital space, especially the internet to democracy are not automatic, neither are they universal. This is because a scrutiny on the government's performance does not spontaneously attract a pro-democratic ripple effect from the citizens. Referring to an experiment conducted in Tanzania in 2010 during the presidential election, Bailard notes that although the internet provided sufficient information to the electorates to interrogate the integrity of election process, a probability of the citizenry not taking part in the elections was reported. On the other hand, the Bosnia and Herzegovina, the internet made the electorates more aware of the importance of quality democracy in their country. With this, the study opines that the internet presents a paradoxical situation to democracy and the democratization process (Bailard, 2014).

Subsequently, while technology was meant to enhance democracy and emphasize on its credibility, new challenges have emerged. Through the use of social media, massive volumes of propaganda have been distributed instantly to the masses. Both state and non-state actors taking advantage of the open nature of the internet to influence public opinion before and during elections. Deploying different forms of cyberattacks, free and fair elections could be disrupted. Ways in which elections could be influenced include manipulating public opinion or influencing it to vote for or against particular parties through a mix of cyber and information operations (Codreanu, 2021). Additionally, malicious actors could also influence in a more direct way the voting process, for instance by hacking into the online features of the voting process and interfere with the voter registration process or by altering the results. However, some of these cyber operations are not only a threat to the democratic process, as they can culminate to physical threats to not only the state but also to individuals (Codreanu, 2021).

The challenges of technology to democracy as mentioned above are massive. Therefore, mitigation strategies are central to ensure the preservation of democracy within states. This study therefore focuses on cyber security strategies to limit the implications of technology and its related innovations to the Kenyan democracy. It interrogates how technology has been used to undermine the Kenyan democracy along with the implications. The different forms of manipulation such as disinformation, deep fake and targeted ads are extensively discussed. At the tail end, the study proposes some cyber security measures to mitigate the possibilities of technology misuse in future elections and to ensure that it is used for the good of the citizenry.

1.2 Research Objective

- (i) Identify how technology has been exploited to undermine the Kenyan democracy.
- (ii) Discuss the effects of the misuse of technology to the Kenyan Democracy.
- (iii) Propose cyber security measure to mitigate the misuse of technology in undermining the Kenyan democracy.

II. LITERATURE REVIEW

2.1 Theoretical Review

2.1.1 Agenda Setting Theory

The agenda-setting role of the media can be traced back to Walter Lippmann's Public Opinion of 1922 where he argued that the news media regulated our global imagination with regards to public affairs without having to directly experience it. In his view, Lippman contends that "*whatever we believe to be a true picture, we treat as if it were the environment itself*" (Lippmann, 1965). Nevertheless, the theoretical aspect of the media's influence on public perception was formalized in 1972 during a seminal presentation where Maxwell McCombs and Donald Shaw proposed the agenda setting theory to illustrate the relation that existed between media emphasis on specific issues and the importance accorded to it by the public. The Chapel Hill study theorized the ability of the media to determine or manipulate the public view on issues considered as important (Almakaty, 2024). This was done by evaluating the extent in which key issues during the 1968 presidential campaign in the US as advanced by the media corresponded to the importance accorded by the voters (McCombs, 2005). And since the media was the most preferred medium for political candidates reaching out to the people, the vast amount of information available in the media was seen as critical for voting decisions (McCombs & Shaw, 1972).



The core tenet of agenda setting posits that issues on public affairs, relating to both election and non-election settings, salient in the media, become eminent among the public (McCombs, 2005). The hypothesis implies that the prominence of issues highlighted on the media's agenda shaped the prominence of the same issues onto the public's agenda. Hence, in choosing and displaying news, editors and broadcasters influence politics as the audience are able to assign importance of issues with regards to the amount of information available (McCombs & Shaw, 1972). And by focusing on a handful of issues, the media subtly attach importance to issues shared. Thus, by determining what is to be seen and supported, Samatan et al. (2024) indicate that the media doesn't tell its audience on what exactly to think, but direct them on what to think about. In this case, Neuman et al. (2014) label "what to think" as a symbol signifying the old blue print on the art of persuasion and attitude change. However, as McCombs (2011) notes, the efforts by the media to influence public opinion are not deliberate or premeditated. Instead, these are simply outcomes for the need of the media to only focus on key topics to be featured.

In the digital age with the proliferation of digital media, especially social media platforms, the traditional dynamics of agenda setting evolved. New actors and mechanisms into the agenda setting process were introduced, meddling with the simple relationship that existed between the media and the public during the inception of the concept. And with the decentralized and interactive nature of social media platforms, users are not only allowed to consume but also create and share content (Almakaty, 2024). This shift therefore not only blurs the lines between media producers and consumers, but also allows a multi directional process of agenda setting. Further, this democratization of information has enabled new challenges in the form of misinformation, disinformation and fake news, with limited chances of information verification. Therefore, as audience increasingly curate their own information environments, the ability of any single entity to set a universal agenda diminishes. Thus, the current information overload necessitates the need for filter bubbles to curate specificity in the delivery of agendas (Almakaty, 2024).

Additionally, online platforms are not only being used for mobilization and self-promotion, but also setting public agenda. This is achieved through the live options on the wide range of the available social media platforms such as Facebook and Instagram live broadcast, where interview footages and statements are released to the news media, and posts and tweets are curated to intervene and contribute to public debates. Candidates and political parties have also adopted a communication strategy where social media platforms are used in familiarizing their policies and agendas (Bentivegna et al., 2022). Thus, with an evolving digital media, the dynamics of setting agendas have become intricate, especially with the online presence of both traditional and social media making them accessible for trend analysis (Neuman et al., 2014).

2.2 Empirical Review

The internet's very low entry barriers allow interactions from anyone and everyone. But as its position in the society balloons, uncertainty surrounds its control, use and management. Presently, as noted by Ren (2024), platforms such as Google, Facebook and YouTube control the advertising market. Consequently, these platforms have turned out to be hosts to politically instigated parties shaping political campaigns (Kornbluh et al., 2020). Making use of malware, targeted ads and algorithms by exploiting user data, these platforms have been used to spread disinformation in addition to targeted ads with the intention of user manipulation (Kornbluh et al., 2020). This not only jeopardizes the functioning of key institutions as Kornbluh et al. (2020) observe, it undermines the rule of law as well as democracy. Additionally, Dan and Pandey (2024) contend, it challenges the sovereignty and state security when foreign entities or non-state actors create chaos through disinformation or election manipulation.

Technological threats to democracy take a number of forms ranging from the manipulation of voters through disinformation and fake news, to the targeting and destruction of particular candidates name, the creation of fake groups to generate and aggravate conflict, and the creation of chaos and disruption to discredit the democratic model (Nye Jr., 2019). Four key ways in which elections could be interfered with through the cyber space are highlighted in a study by Kamau and Shiundu, (2024). First, through vote manipulation, secondly through massive manipulation of the opinions influencing the vote, third by tampering with the voting process and lastly by sabotaging the confidence in as far as the integrity of the votes are concerned. At present, social media has presented itself as a double-edged sword. Despite the fact that it has provided a more inclusive involvement of citizens in public deliberations, it has been used for malicious activities, (Codreanu, 2021). Its ability to make information readily available has presented opportunities for manipulation, hence being dubbed 'sharp power' (Cheng et al., 2018).

Whereas technology and social media platforms were initially politicised in the Arab Spring campaign and used as tools for democracy, they have since been remodeled and taken a threatening dimension in numerous territories. These sites have not only deepened precarious and reckless speech but also heightened emotional ethnic discussions that could be used to destabilize a country peace. By obstructing democracy, political elites within states have been able to increase their political mileage (Gopaldas, 2019). Although the positives associated with social media such as promoting transparency and accountability between governments and its citizens still exist, a number of risks have since emerged. For instance, in the wake of the Cambridge Analytica saga, Facebook was largely viewed as a threat to



democracy as a result of its negligence towards regulating fake news in both the Brexit vote and the US election in 2016 (Solon, 2016).

In their study on cyber threats to democratic processes, Siman-Tov et al. (2017) categorize cyber threats that undermine democracy of states into two ; Cyber threats that are likely to throw into disarray the democratic process by use of technological tools devised to interfere with not only the polling and voting system but the integrity of these systems and secondly, material threats to the democratic institutions in place by means of tarnishing their reputation and eroding the public's confidence. The interruption of democratic process can be done via a number of cyber operations as well as online information operation. A cyber operation involves an array of clandestine activities executed through the digital infrastructure in order to gain unauthorized access to a system for the purposes of compromising its services, data manipulation or espionage, while information operation is carried out on the online information setting to secretly distort, confuse, mislead or manipulate a targeted population through deceptive or inaccurate information (O'Connor et al., 2020).

In a study focusing on foreign interference in domestic politics, Cheong et al. (2020) highlight that the growth of Information and Communications Technologies (ICTs) has accelerated the sophistication of foreign interference in domestic politics. It has facilitated refined models in which an earmarked state can be manipulated as well as empower adversaries towards the development of techniques to conceal their activities. The main intention of foreign interference as Peck (2024) observes, especially in the electoral process of a targeted state is to create doubts to the integrity of the process and the state's democratic institutions. In October 25th 2024 for instance, the US Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) issued a communiqué indicating that Russian actors were behind a trending video portraying an individual tearing up ballots in the state of Pennsylvania. The intentions of the video as per the communiqué was to question the integrity of the US elections as well as stir up divisions among the American population (*Joint ODNI, FBI, and CISA Statement*, 2024).

Cade et al. (2024) highlight three key objectives in as far as the drivers to elections interference are concerned. First is the need for influence. Whether a foreign state or cyber criminals working for monetary gain, need for influence is key. In this case, strategies such as misinformation and disinformation campaigns are carried out especially on social media platforms in order to sway public opinion. The second objective is the need to disrupt. By attacking electoral infrastructure, physical impacts that could interfere with election activities hence damaging the integrity of critical databases is likely to be achieved. In certain cases, these attacks could result in the population being unable to vote. The third and last objective of election interference is the need to undermine. Through cyber-attacks or misinformation and disinformation, the public trust to the whole electoral process could be undermined. The key agenda is to wear down the trust the citizenry holds on the existing democratic process as well as the institution spearheading it. And this could be accomplished via something as simple as a defaced web page.

Since the foreign electoral interference of the 2016 US presidential elections therefore, digital platforms such as Facebook and X formerly Twitter have instigated new policies along with intrinsic functionalities to counter disinformation and foreign interferences to the democracy of states (Kornbluh et al., 2020). X for instance forbids the suppression of information and practices that could interfere with the experience of other users on the platform(Tan, 2022). Such practices include impersonation, election interference with the intention of misleading other users, failure to which a user receives a warning of the content is barred from being shared all together. To identify such contents, X depends on its users to report such content. Similarly, Facebook depends on its users to report offensive or false content. Once a user submits a report, it is scrutinized for any violations of the Facebook's community standards(Tan, 2022). Further, through a fact checking program initiated in December 2016, potentially fake information is identified via other user's feedback through the various third-party fact-checkers certified through a non-partisan International Fact-Checking Network. The fact-checkers review content, and rate its accuracy. The distribution of any inaccurate content is reduced so that fewer people can see it(*How Meta's Third-Party Fact-Checking Program Works*, 2021). Currently, the program includes more than 90 organizations working in more than 60 languages globally.

III. METHODOLOGY

This study seeks to highlight how technology has impacted the Kenyan democracy and propose cyber security measures to mitigate against its negatives. The study employs a desktop review of existing literature collected from online academic databases using the study's key words. Other documents such as reports were collected from the respective organizations' online library. Literature published in English from high impact journals from the social sciences field were prioritized. Considering the fluidity of the topic under review, studies carried out within the past ten years were preferred. To ensure the credibility of the data and avert misrepresentation of facts, both qualitative and quantitative secondary data were considered for analysis in answering the research questions. For data analysis, content related to this study was collected, categorized, analyzed and then organized into the various subjects associated with



the research questions. The findings are categorized thematically on the key issues associated with the use of technology on the Kenyan democratic process, with the discussion focusing on an analytical interpretation of the findings. This structured approach ensures ethics and neutrality is maintained.

IV. FINDINGS & DISCUSSION

4.1 Response Rate

4.1.1 Disinformation, Fake News in Election Deceit

Fake news is the intentional presentation of deceitful information posing as legitimate news (Nye Jr., 2019). It could also be viewed as information that is untrue, but being published as authentic news, either deliberately or by accident (Portland Africa, 2017). In cases where false information is deliberately shared for the purposes of misleading the population, this is categorized as an act of disinforming. Wardle and Derakhshan define disinformation as the deliberate creation and spreading of false information with the intentions of creating harm to a person, a group of people or an organization (Wardle & Derakhshan, 2017). Fake news and disinformation have been observed to trend effortlessly, with speed and at very minimal costs (Nye Jr., 2019), an environment put forward by the massive use of the internet. Kenya has not only been ranked among Africa's top countries in smartphone penetration and social media usage (Kamau & Shiundu, 2024), it has also experienced a rapid growth in the use of the internet (Cheng et al., 2018). As at January 2023, the country recorded over 17.86 million internet users and 10.55 million social media users, representing 19.3 percent of the total population (Kemp, 2023). This has been observed to aggravate the spread of misinformation and disinformation especially during the election period.

Fake news and disinformation became a focus of attention in Kenya in April 2017, when a fake front page of one of the dailies was circulated, claiming that a gubernatorial aspirant vying under one of the opposition parties had defected to the ruling party. The main aim behind the spread of the fake news was to discredit the aspirant on the day of the nomination (Mayoyo, 2017). Additionally, during the 2022 elections period, Madung (2022), analyzing a sample of 132 videos on Kenyan TikTok noted the platform was massively used to disseminate propaganda, hate speech and disinformation by spreading untrue claims on various candidates and threatening some ethnic communities. The fake news menace is affirmed by a research by Portland Africa, a communications consultancy, that revealed that fake news is a pervasive problem surrounding the Kenyan elections with 90% of respondents having seen false or inaccurate information and 87% viewing this information as being deliberately false (Portland Africa, 2017). Additionally, with 48.4 percent of social media users in Kenya depending on social media platforms for news update (Mboya, 2024), these platform have become fertile grounds for information manipulation.

And unlike the 2013 and 2017 general elections where external actors were known to be active as evidenced by the Cambridge Analytica revelations, the August 2022 campaign period established that influence operations were primarily local and homegrown, demonstrating that this capacity has been developed locally. Numerous misleading information was shared on various social media platforms with the intention of suppressing the voters. Claims of wild animals on the loose were reported within certain regions, as well as military deployment within the capital just to mention but a few. The dissemination of disinformation was majorly done through fake polls, fake news sites, in addition to pseudo social media accounts impersonating individuals and groups, sharing information on social sites such as Twitter and TikTok abusing algorithms to intensify the spread of disinformation. Prior to the August 2022 general elections, as a result of a surge in deceptive articles within Nyeri County, a research on the role of social media in the spread of fake news put Facebook and Twitter as the platforms with the highest rate of fake news, with 87 percent and 72 percent respectively. This can be attributed to the fact that a significant majority of participants opined that social media is readily available to a wide demographic, especially those who own smartphones. Through these sites, information dissemination, both genuine and false were instant hence ideal (Munene & Oloo, 2024).

4.1.2 Cyber Operations and Foreign Interference

The most ideal technique to taint the democratic process is through the manipulation of the electoral system. This can be achieved by hacking either in to the voting system or the voters register (Nye Jr., 2019). Over the past decade, state actors have taken advantage of the digitisation of electoral systems, election administration and election campaigns to interfere in foreign elections and referendums. Their activities can be divided into two attack vectors. First, they've used various cyber operations, such as denial of service (DoS) and phishing attacks, to disrupt voting infrastructure and target electronic and online voting, including vote tabulation. Secondly, they've used online information operations to exploit the digital presence of election campaigns, politicians, journalists and voters (O'Connor et al., 2020). With the proliferation of technology, it's become quite easy for adversaries to target politicians and their allies through mobile spyware tools (Memon & Awan, 2017). During the Kenya's 2022 general elections for instance, an Israeli disinformation specialist is alleged to have hacked into various accounts of three close aides to a presidential candidate (Stephanie & Jason, 2023). During a demonstration to journalists posing as potential clients, the hack is said



to involve an infiltration of Gmail and Telegram accounts. The specialist is alleged to have sent messages without the user's knowledge on telegram with the intention of creating confusion during the campaigns.

4.1.3 Data and Targeted Campaigns

The proliferation of technology has transformed data to an increasingly valuable commodity with entities competing on who controls what (Hankey et al., 2018). Since the Cambridge Analytica and the Facebook saga, the exploitation of data has been a key topic in most quarters, owing to the fact that it has been able to transform modern campaigns. Used along with artificial intelligence, data has made available the perfect environment for microtargeting of information, with every individual's information closed in some form of a filter bubble. Further, social networking sites have also encouraged the growth of a profit model where the user is the product and their information shared with third parties such as advertisers. Making use of algorithms, users are kept engaged so that more ads are served to them for an extra revenue (Nye Jr., 2019). This cheap nature of digital media has made online campaigns possible (Dwivedi et al., 2021) with the predictive model promising to be more efficient hence leading to successful campaigns (Nickerson & Rogers, 2014). However, despite the impacts of the use of data and microtargeting in the political arena, its regulatory underpinnings have since remained obscure (Hankey et al., 2018).

Unlike in 2013, the 2017 general elections experienced a shift towards a personalized data driven approach (Mutung'u, 2018) exposing a big gap that existed in as far as protecting people's data is concerned. Political parties are said to have hired data mining companies such as the Cambridge Analytica who developed microtargeting strategies using public opinion platforms to create content such as memes that would be shared mainly through social sites (Mutung'u, 2019). Parties, along with their candidates made use of targeted advertising especially on social media as a move to diversify from the traditional forms of advertising. Using Google ads, disinformation was rapidly spread to the masses. Moreover, there was an increase in the use of personalized SMS by aspirants as well as their respective parties. Voters especially within urban areas received personalized text messages from respective aspirants within their constituencies seeking their votes. Supporters were further organized in WhatsApp groups and Telegram channels to enhance communication. This was mostly done without the consent of the constituents added to the groups (Mutung'u, 2018). Further, there was a rapid increase in the use of bulk SMS texting that was targeted at particular constituents and unsolicited messaging seeking votes (Mosero, 2022).

The key values in relation to data privacy as stipulated in the Data Protection Act 2019 include confidentiality, integrity, accountability, and transparency (Masibo, 2022). To ensure data transparency during elections, the KIEMS kits were introduced. They include the Biometric Voter Registration System (BVR) used for voter identification at the polling station as well as results transmission system software that restricts the election officials from transmitting results with figures more than registered voters at any polling station. The BVR is able to capture a voter's facial image, fingerprints and civil data and was first deployed in 2013 (Masibo, 2022). Although the KIEMS kits were intended to enhance the electoral process, as well as increase transparency, concerns emerged after some of the data collected for voter registration was used for canvassing for political support and political campaigning (Mosero, 2022). After the publishing of respective party members online by the Registrar of Political Parties as required by law, many citizens were shocked to find themselves registered as members of political parties without their knowledge (Mutung'u, 2018). As a result, questions emerged on how safe the data collected during the voter registration is, bringing up the possibilities of these data being misused or manipulated.

4.1.4 Artificial Intelligence and Deep Fake

Artificial Intelligence (AI) and its diverse capabilities has heightened the possibilities of new threats to democracies globally. These threats include the generation of deep fakes which involves the use of algorithms to manipulate a video but still make it look like the original (Temir, 2020). By making use of AI, deep fakes depict an individual in a certain way as intended by the creator of the video. In many countries, deep fakes are not illegal, however depending on the context of the video created, they could not only infringe on the copy right but also data privacy as well as damage a person's or an organization's reputation (Ngila, 2021).

Elections allow voters to elect leaders of their choice, hence when untrue information about their leader of choice is shared, the voter's choice is likely affected (Kigwiru, 2022). Just a week to the 2017 general elections, two videos purporting to originate from two international media houses emerged. Both videos indicated that the incumbent president was leading in the polls (Sevenzo, 2017). Although the sources of these videos were never identified, the videos are believed to have first been sent via WhatsApp and slowly went viral on other social networking sites. By the same token, in 2022, videos emerged of two presidential candidates where in one, subtitles were manipulated to depict the candidate hurling threats in his local dialect to non-members of his local tribe while the other was a fake audio claiming to be a leaked phone call between the secretary-general of a coalition party, and an official of the electoral body attempting to rig the elections (Owino, 2022). These fake videos could not only act as catalysts of ethnic strife, a



challenge that Kenya as a country is still grappling with, but also lack of confidence to the electoral body in charge of elections in the country.

4.2 Discussion

The key pointer to an effective democratic governance is where power has been entrusted to the people (Ezrachi & Robertson, 2024). For this to happen, a free flow of undistorted information is paramount to enable the citizens to make their independent choices. Through the emergence of digital technologies and online platforms, a wide range of information sources have been realized hence enhancing the democratic process of states. The introduction of technology into the Kenyan electoral process was meant to improve efficiency and effectiveness and also mitigate against election fraud that led to the 2007 post-election violence. Making use of social media platforms, information sharing was enhanced with the public easily taking part in political debates along with private or public communications among citizens. The plurality of information has however opened doors for an increased manipulation, disinformation, and distortions of information not only in the market place but also in the political arena (Ezrachi & Robertson, 2024).

The wide spread use of disinformation, fake news and deep fake strategies during the 2017 and the 2022 Kenyan general elections points towards the immense control that big tech companies such as Google, Amazon, Meta etc. have over political communication and mobilization (Fukuyama et al., 2021). This can be attributed to the fact that these companies are the key disseminators of information and consequently, pose a huge threat to democracy. Through social media platforms, fake news in addition to conspiracy theories were effortlessly pushed forward. Further, making use of algorithms, filter bubbles specific to previous users' searches were created. With this, political voices were either heightened or subdued thus having massive influence on democratic political debate. Thus, as we move our lives online, we grant these platforms so much power that they can either knowingly, or unknowingly manipulate elections in any given territory.

To avoid a repeat of the 2007-2008 post elections violence, under the recommendations of the Krigler commission¹, the Kenyan government was able to first digitize the electoral process in the 2013 general elections, which was unsuccessful as a result of system failure (Bowman & Longwe, 2013). Learning from the challenges encountered, an improvement was made during the 2017 elections, paving way to the introduction of the Kenya Integrated Election Management System (KIEMS) that consists of the Biometric Voter Registration (BVR), Electronic Voter Identification (EVID), and the Results Transmission System (RTS) to be used during tallying (Omwoha, 2022). While digital technologies were introduced to gain the trust of the electorates, Omwoha (2022) observes that the more technological aspects were included to the electoral system, the more the citizens developed mistrust towards the administrative systems. The access and misuse of voters' data raised questions on the credibility and integrity of the systems put in place to ideally streamline the electoral process. As a result, digital technologies have elicited the impression of destabilizing the process of participatory democracy.

The incorporation of technology such as the KIEMs kit in the electoral process is not a cheap affair. In 2022 for instance, the Kenyan election cost approximately Ksh.44 billion (Mutai, 2022), making it the second most expensive election in the country's history (Mutinda, n.d.). Thus, the high costs of election technology have increased the dependencies of African states, Kenya included to foreign support in running elections. This therefore raises questions on the role of external actors for instance liberal institutions such as United Nations Development Programme (UNDP) whose activities on democracy promotion are evident (*The Role of UNDP in Supporting Democratic Elections in Africa*, 2015). This as Jacobsen (2020) argues, is a typical representation of democracy assistance. Simply put, democracy assistance involves working with institutions, public officials as well as the citizens for the sole purpose of promoting democratic governance along with its elements such as participation, fair elections, inclusion, just to mention but a few (Black, 2019). Although democratization is ideally homegrown, Black (2019) asserts that through democracy assistance in the form of foreign grants, players in host countries can be bolstered up to alleviate oppression, enhance democracy as well as improve quality of life. And although democracy assistance is not expected to be biased, depending on its nature and institutions involved, it is sometimes viewed as one sided hence seen as opposing and threatening to the ruling elites.

At present, Kenya has put in place a number of strategies and mitigations in order to protect the electoral process against the threat of election interference. Among key recommendations, the Election (Technology) Regulation of 2017 posits the annual audits of the election technology, or as may be required, to not only guarantee data integrity but also to ensure that the electoral technology in place functions effectively as specified along with its internal controls (The Elections (Technology) Regulations, 2017 Arrangement of Regulations, 2017). Additionally, the enactment of the Computer Misuse and Cyber Crimes Act of 2018 has been able to strengthen a multi-agency collaboration framework

¹The Krigler Commission, officially The Independent Review Commission (IREC), was an international commission of inquiry established by the Government of Kenya in February 2008 to Inquire into all aspects of the 2007 General elections with particular emphasis on the presidential elections.



in order to contribute to the national cyber security resilience (*Cyber Security | Communications Authority of Kenya*, n.d.). Despite the above-mentioned mitigation to guard against election interferences, the country is still grappling with the use and misuse of technology in democratic manipulation. Although many may insist that election technology can be fully protected, cybersecurity experts generally agree that there is no way to guarantee an absolute level of security against cyber threats and fully protect against all risks. While cybersecurity risks cannot be eliminated entirely, many can be mitigated with the application of security controls as part of a holistic cybersecurity strategy (Boyce et al., 2023).

V. CONCLUSION & RECOMMENDATIONS

5.1 Conclusion

The proliferation of technology has transformed many aspects of life among the Kenyan populace. They include information dissemination which is crucial in exercising democracy. In order to ensure data availability, accuracy, integrity, and confidentiality of the electoral process, a number of legislations were adopted. This came along with the incorporation of technology in the voter registration phase, identification and transmission of results during elections. This notwithstanding, the process has experienced numerous challenges some of which led to the nullification of the 2017 presidential elections. Conversely, with a majority of the citizens depending on social media platforms for information, the political class and their allies have found ways to manipulate information to their advantage. This in many ways has interfered with the democratic process. To mitigate its negative implications, functional cyber security measures need to be put in place. While this may not totally eliminate emerging cyber threats, it is likely to eliminate the most vulnerable low hanging fruit.

5.2 Recommendations

There is need to enhance algorithmic accountability with companies required to monitor their systems more effectively and in a publicly more accountable manner. By regulating social media ads, the quality of information sharing via social media platforms would be bound by some form of regulation hence liable to mitigations in cases where non-compliance is reported.

It is critical that private entities within the internet environment come up with means, products and systems for protecting citizens from intrusions by states and non-state actors. This includes policies governing online content agreed upon by all stakeholder and are in line with International Human Rights law that include freedom of expression and right to privacy. Further, there is need to assume more accountability by enacting regulations to safeguard against the dissemination of false information. This might include identifying and marking false information and enforcing strict punishments for those who disseminate propaganda online.

In order to protect the election infrastructure against threat actors both state and non-state, homegrown and foreign actors, it is recommended that the adopted election technology in Kenya, along with its equipment be categorized as critical infrastructure. This, will open up the election systems to receive additional government assistance with the cyber security protection of the electoral systems beefed up. To ensure the integrity of elections, Kenya needs to update its election systems and use devices on an independent network that is sufficiently backed up using modern technologies. Further, it's important to have cybersecurity continuously updated for sensitive systems related to voter registration lists, voting, and results tabulation.

Through a public – private partnership, stakeholders could come up with cyber security awareness drives on emerging threats in addition to provide guidance for businesses and the general public. By focusing on efficacy, the voters trust is likely to be restored. Additionally, it is vital to liaise with political leaders informing them of the existing cyber risks. With this, political parties, their candidates and staff will become more alert on the importance of basic cyber hygiene such as encryption and multifactor authentication.

REFERENCES

- Almakaty, S. (2024). Agenda setting theory in the age of digital media: An analytical perspective. *Evolutionary Studies in Imaginative Culture*, 8(4), 1742–1750. <https://doi.org/10.70082/esiculture.vi.1539>
- Bailard, C. S. (2014). *Democracy's double-edged sword: How Internet use changes citizens' views of their government*. JHU Press.
- Bentivegna, S., Marchetti, R., & Stanziano, A. (2022). The agenda-building power of Facebook and Twitter: The case of the 2018 Italian general election. In D. Taras & R. Davis (Eds.), *Electoral campaigns, media, and the new world of digital politics* (pp. 124–142). University of Michigan Press. <http://www.jstor.org/stable/10.3998/mpub.12013603.9>
- Berg, S., Staemmler, D., & Thiel, T. (2022). Political theory of the digital constellation. *Zeitschrift Für Politikwissenschaft*, 32(2), 251–265. <https://doi.org/10.1007/s41358-022-00324-4>



- Black, D. (2019). *Revitalizing democracy assistance to counter threats to democratization*. German Marshall Fund of the United States. <http://www.jstor.org/stable/resrep21221>
- Bowman, W., & Longwe, B. M. (2013, March 29). Technology, transparency, and the Kenyan general election of 2013. *Al Jazeera*. <https://www.aljazeera.com/opinions/2013/3/29/technology-transparency-and-the-kenyan-general-election-of-2013>
- Boyce, S., Martin-Rozumilowicz, B., Darnolf, S., Dreher, C., Ellena, K., Polk, B., Roitman, F., Scott, V., Shein, E., & Vickery, C. (2023). *Understanding cybersecurity throughout the electoral process: A reference document. An overview of cyber threats and vulnerabilities in elections*. https://www.ifes.org/sites/default/files/2023-06/Understanding-Cybersecurity-Throughout-the-Electoral-Process_1.pdf
- Brooke, H. (2016). Inside the digital revolution. *Journal of International Affairs*, 70(1), 29–53. <https://www.jstor.org/stable/90012596>
- Cade, J., Simmons, G., & Thomson, S. (2024, February 20). The cyber impact on elections: Safeguarding democracy in 2024. *BAE Systems Digital Intelligence*. <https://www.baesystems.com/en/blog/the-cyber-impact-on-elections-safeguarding-democracy-in-2024>
- Cheng, Q., Cunningham, C., Gacayan, F., Gu, A., Hall, A., Lee, O., Sawyer, A., Sayoud, S., Wadhwa, V., & Yi, J. (2018). *Hacking democracy: Cybersecurity and global election interference*. <http://hdl.handle.net/1773/43754>
- Cheong, D. D., Neubronner, S., & Ramakrishna, K. (2020). Foreign interference in domestic politics: A national security perspective. *S. Rajaratnam School of International Studies*. <http://www.jstor.org/stable/resrep24326>
- Codreanu, C. M. (2021). Digital democracy in peril: Safeguarding e-democracy by boosting cybersecurity. *Smart Cities International Conference (SCIC) Proceedings*, 9, 461–474. <https://www.scrd.eu/index.php/scic/article/view/387>
- Communications Authority of Kenya. (n.d.). Cyber security. Retrieved September 15, 2024, from <https://www.ca.go.ke/cyber-security>
- Dan, V., & Pandey, M. (2024). Cyber-security threats in international relation: The implications of cyber threats on state sovereignty, national security, and international cooperation, focusing on recent cyber incidents rational analysis in geographical point of view. *International Journal of Creative Research Thoughts*, 12, 2320–2882. <http://www.ijcrt.org>
- Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluto, H., Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, P. A., Rowley, J., Salo, J., Tran, G. A., & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, 59, 102168. <https://doi.org/10.1016/j.ijinfomgt.2020.102168>
- Ezrachi, A., & Robertson, V. H. S. E. (2024). Can competition law save democracy? Reflections on democracy's tech-driven decline and how to stop it. *Journal of Antitrust Enforcement*. <https://doi.org/10.1093/jaenfo/jnae043>
- Fukuyama, F., Richman, B., & Goel, A. (2021). How to save democracy from technology: Ending big tech's information monopoly. *Foreign Affairs*, 100, 98.
- Gopaldas, R. (2019). Digital dictatorship versus digital democracy in Africa. *South African Institute of International Affairs*. <http://www.jstor.org/stable/resrep25956>
- Gorokhovskaia, Y., & Grothe, C. (2024). *Freedom in the world 2024: The mounting damage of flawed elections and armed conflict*. <https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict>
- Hankey, S., Marrison, J. K., & Naik, R. (2018). Data and democracy in the digital age. *The Constitution Society*. <https://consoc.org.uk/publications/data-and-democracy-in-the-digital-age/>
- Jacobsen, K. L. (2020). Biometric voter registration. *Cooperation and Conflict*, 55(1), 127–148. <https://www.jstor.org/stable/48552823>
- Joint ODNI, FBI, and CISA Statement. (2024). *CyberSecurity & Security Agency*. <https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement-0>
- Kamau, S., & Shiundu, A. (2024). Investing in fake news? The disinformation industry in Kenya's 2022 elections. In *State-sponsored disinformation around the globe* (pp. 194–215).
- Kemp, S. (2023, February 13). Digital 2023: Kenya — DataReportal – Global Digital Insights. *DataReportal*. <https://datareportal.com/reports/digital-2023-kenya>
- Kigwiru, V. K. (2022). Deepfake technology and elections in Kenya: Can legislation combat the harm posed by deepfakes? *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.4229272>
- Kornbluh, K., Goodman, E. P., & Weiner, E. (2020). Safeguarding digital democracy. *German Marshall Fund of the United States*. <http://www.jstor.org/stable/resrep24545>
- Lippmann, W. (1965). *Public opinion* (Original work published 1922). <http://infomotions.com/etexts/gutenberg/dirs/etext04/pbpnn10.htm>



- Madung, O. (2022). From dance app to political mercenary: How disinformation on TikTok gaslights political tensions in Kenya. *Mozilla Foundation*. <https://www.mozillafoundation.org/en/campaigns/kenya-tiktok/>
- Masibo, M. (2022, September 15). Safeguarding personal data during Kenya's 2022 general election. *KICTANet Think Tank*. <https://www.kictanet.or.ke/safeguarding-personal-data-during-kenyas-2022-general-election/>
- Mayoyo, P. (2017). Fake news by bloggers could mess Kenya's 2017 elections. *Standard Media*. <https://www.standardmedia.co.ke/business/article/2001237115/fake-news-by-bloggers-could-mess-2017-elections>
- Mboya, T. (2024, February 6). Rise in disinformation and influence operations: Kenyans beware. *The Elephant*. <https://www.theelephant.info/opinion/2024/02/06/rise-in-disinformation-and-influence-operations-kenyans-beware/>
- McCombs, M. (2005). A look at agenda-setting: Past, present and future. *Journalism Studies*, 6(4), 543–557.
- McCombs, M. (2011). *The news and public opinion: Media effects on civic life*. Polity Press.
- McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *The Public Opinion Quarterly*, 36(2), 176–187. <http://www.jstor.org/stable/2747787>
- Memon, S., & Awan, J. H. (2017). *Handbook of cyber-development, cyber-democracy, and cyber-defense*. <https://doi.org/10.1007/978-3-319-06091-0>
- Meta. (2021, June 1). How Meta's third-party fact-checking program works. <https://www.facebook.com/formedia/blog/third-party-fact-checking-how-it-works>
- Mosero, R. (2022). In Kenya's 2022 elections, technology and data protection must go hand-in-hand. *Carnegie Endowment for International Peace*, August, 1–6. <https://carnegieendowment.org/2022/08/08/in-kenya-s-2022-elections-technology-and-data-protection-must-go-hand-in-hand-pub-87647>
- Munene, M. M., & Oloo, D. (2024). Role of social media platforms in the spread of fake news in Nyeri County, Kenya. *African Journal of Empirical Research*, 5(2), 229–239. <https://doi.org/10.51867/ajernet.5.2.21>
- Mutai, E. (2022, August 10). The hidden costs that make Kenya polls money guzzlers. *Business Daily*. <https://www.businessdailyafrica.com/bd/data-hub/the-hidden-costs-that-make-kenya-polls-money-guzzlers-3922944>
- Mutinda, L. (n.d.). 2022, Kenya's second most expensive election. *Debunk Media*. Retrieved November 6, 2024, from <https://debunk.media/2022-kenyas-second-most-expensive-election/>
- Mutung'u, G. (2018). The influence industry: Data and digital election campaigning in Kenya. *Our Data Ourselves*. <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf>
- Mutung'u, G. (2019, January 21). Kenyans must defend their digital rights. *DW Akademie*. <https://akademie.dw.com/en/kenyans-must-defend-their-digital-rights/a-47133164>
- Neuman, R. W., Guggenheim, L., Mo Jang, S., & Bae, S. Y. (2014). The dynamics of public attention: Agenda-setting theory meets big data. *Journal of Communication*, 64(2), 193–214.
- Ngila, F. (2021, March 14). How deepfakes could make Kenyan politics murkier. *Nation*. <https://nation.africa/kenya/business/technology/how-deepfakes-could-make-kenyan-politics-murkier--3322238>
- Nickerson, D. W., & Rogers, T. (2014). Political campaigns and big data. *Journal of Economic Perspectives*, 28(2), 51–74. <https://doi.org/10.1257/jep.28.2.51>
- Nye Jr., J. S. (2019). Protecting democracy in an era of cyber information war. *Belfer Center for Science and International Affairs*, February. <https://www.belfercenter.org/sites/default/files/files/publication/ProtectingDemocracy.pdf>
- O'Connor, S., Hanson, F., Currey, E., & Beattie, T. (2020). Cyber-enabled foreign interference in elections and referendums: Policy brief. *The Australian Strategic Policy Institute Limited*, 41. www.aspi.org.au
- Omwoha, J. (2022). 'Open the Servers.' *Africa Development / Afrique et Développement*, 47(2), 147–160. <https://www.jstor.org/stable/48682669>
- Owino, V. (2022, August 6). Kenya election: Deep fakes, propaganda, libel inundate social media. *The East African*. <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-election-deep-fakes-propaganda-inundate-social-media-3904934>
- Peck, S. (2024). Foreign election interference. *Harvard Model Congress 2024*. <https://static1.squarespace.com/static/5cb7e5637d0c9145fa68863e/t/654970f1f350f73fb7d72f1a/1699311857567/HMC2024+Senate+Intelligence+2.pdf>
- Portland Africa. (2017). *The reality of fake news in Kenya*. <https://portland-communications.com/publications/reality-fake-news-kenya/>
- Ren, Q. (2024). Advertising and content creation on digital content platforms. *Marketing Science*, 43(4), 734–750.



- Samatan, N., Nurhasanah, N., Londol, M., Robingah, R., & Fania, S. (2024). Critical discourse network analysis on Ferdy Sambo news in online media using agenda setting theory. *Jurnal Komunikasi Ikatan Sarjana Komunikasi Indonesia*, 9(1), 146–167.
- Sevenzo, F. (2017, July 31). Kenya election: Fake CNN, BBC reports target voters. *CNN*. <https://edition.cnn.com/2017/07/31/africa/kenya-election-fake-news/index.html>
- Siman-Tov, D., Siboni, G., & Arelle, G. (2017). Cyber threats to democratic processes. *Cyber, Intelligence, and Security*, 1(3), 51–63.
- Solon, O. (2016, November 10). Facebook’s failure: Did fake news and polarized politics get Trump elected? *The Guardian*. <https://www.theguardian.com/technology/2016/nov/10/facebook-fake-news-election-conspiracy-theories>
- Stephanie, K., & Jason, B. (2023, February 15). Political aides hacked by ‘Team Jorge’ in run-up to Kenyan election. *The Guardian*. <https://www.theguardian.com/world/2023/feb/15/political-aides-hacked-by-team-jorge-in-run-up-to-kenyan-election>
- Tan, C. (2022). Regulating disinformation on Twitter and Facebook. *Griffith Law Review*, 31(4), 513–536. <https://doi.org/10.1080/10383441.2022.2138140>
- Temir, E. (2020). Deepfake: New era in the age of disinformation & end of reliable journalism. *Selçuk İletişim*, 13(2), 1009–1024. <https://doi.org/10.18094/josc.685338>
- The Elections (Technology) Regulations, 2017 Arrangement of Regulations, 309 (2017). <http://libraryir.parliament.go.ke/handle/123456789/1635>
- United Nations Development Programme. (2015, November 15). The role of UNDP in supporting democratic elections in Africa. <https://www.undp.org/publications/role-undp-supporting-democratic-elections-africa>
- Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking (Vol. 27). *Council of Europe*. <https://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf>