De-platforming political disinformation in social media: adaptation mechanisms ahead of Kenya's 2022 electioneering period

Dr John Mwangi

Abstract

Facebook's and Twitters' move to block political disinformation on their platforms is bound to render the social media environment to adaptation mechanisms. The de-platforming of key political figures is likely to embolden the rapid rise of new social media applications such as Fire Chat, Signal, Xender and Lantern while boosting the utilisation of the virtual private networks (VPNs) in political disinformation campaigns. The use of alternative social media applications in the run-up to Kenya's 2022 general elections has the potential to negatively impact on the country's national security and cohesion. There is need for policy makers to develop new strategies to counter disinformation and engage in counter-messaging.

Photo Credit: grupoioe.es

Introduction

Political disinformation via social media applications has been a constant feature of the past three Kenyan elections (2007, 2013 & 2017). It can be argued that the use of social media for propaganda and disinformation is not new in election cycles in Kenya (Maweu, 2019). Nonetheless, it is the fluidity of new media applications that is at stake.

The phenomenon involves the use of propaganda, falsehoods and rumors to mislead the electorate and undermine national security. Historically, the phenomenon had been applied in the World War II and the Cold War era majorly through use of fake news spread via clandestine radio stations, newspapers and other media to deceive publics and governments (Shu *et al.*, 2020).

Social media applications have been used to disseminate hate speech and to mobilise political violence in previous electoral cycles (Mutahi & Kimari, 2020). In the 2017 general elections, Facebook, WhatsApp and Twitter were used to spread fake news, especially to create political tensions, persuade voters, and to discredit institutions such as the Judiciary and the Independent Electoral and Boundaries Commission. These strategies worked through 'digital warriors' on both sides of the political divide (Mutahi & Kimari, 2020).

Disinformation through the use of social media especially around electoral cycles remains a critical national security issue. This is further complicated by external actors who may choose to capitalise on internal tensions to launch fake news so as to influence public opinion (Levush, 2020). These impact directly on electoral integrity and trust in democratic institutions. This paper analyses the various adaptations social media users are likely to assume in the wake of tight platform policies and their implications on 2022 electioneering period in Kenya.

Photo Credit: Parent.com

The context

Prior to the 2017 general elections, the Communications Authority of Kenya (CA) together with the National Cohesion and Integration Commission (NCIC) issued guidelines for political messaging on social media platforms. These guidelines emphasised proper language and tone devoid of hate speech, incitement, including truth and accuracy in the messaging (CA & NCIC, 2017). Nonetheless, the guidelines were hardly enforced.

Since March 2020, the Internet landscape has seen extensive changes amidst the COVID-19 pandemic in Kenya. With policies such as working from home, and the rapid demand for virtual meetings, internet penetration has significantly improved mostly due to Kenya growing youth bulge that is tech savvy and with access to the Internet. Data from the Communications Authority of Kenya, the industry regulator, indicates that in the 2018/19 period mobile data/Internet subscription stood at 49,532,380. Out of these 99% were mobile phone subscriptions, with only 1% being fixed Internet subscriptions (CA, 2020). With the 2019 census indicating that youth aged (18-34) comprises 13,777,600 people, there exists a significant demographic that can be easily mobilised for disinformation.

This analysis projects an expanding mobile Internet penetration rate for the country. In addition, the rise of new social media outlets such as FireChat, Signal, Xender, and Lantern will likely to be used in the 2022 general elections for disinformation given their relative abilities to circumvent government regulations. The possibilities of the uptake of VPN networks also mean that disinformation could spread devoid of government control.

Managing political disinformation through the use of social media is emerging as the new normal in the global political arena. Key social media applications (SMAs), Facebook and Twitter, have banned former US-President Trump from their platforms for posts that encouraged violence at the United States Capitol on January 6, 2021. In March 2020, false posts about the Coronavirus from Brazil's president Jair Bolsonaro and Venezuela's president Nicolás Maduro were pulled down. Similarly, an account linked to Iran's supreme leader, Ayatollah Ali Khamenei, was banned after he posted threats to avenge the assassination of former Iranian Military General, Qasem Soleimani. In the run-up to 2021 general elections in Uganda, Facebook removed a network of accounts and pages in Uganda that engaged in what they termed as coordinated inauthentic behavior to target public debate ahead of the election. This move made Uganda to shutdown Facebook, Twitter and WhatsApp indefinitely ahead of the contentious elections thereby offloading the social-media thirsty public to alternative platforms.

Photo Credit: securityboulevard.com

Even though evidence points to significant reduction in disinformation as a result of the bans, 100% success has not been achieved since the environment is rapidly adapting to circumvent the new normal. These applications could be used to spread disinformation during the electioneering period since technological advancements catalyse the spread of propaganda (Vasu et al., 2018).

FaNkews

This paper projects four adaptation strategies that are likely to be used for disinformation; the rise of alternative social media applications, the use of virtual private networks (VPNs), silent penetration of existing social media applications and new media applications. The paper projects that these adaptation mechanisms present several internal security threats ahead of the 2022 General elections. Thereafter, several recommendations on legal and policy interventions are offered.

The rise of alternative social media applications

The build up to 2022 General elections in Kenya is likely to witness an increase in the use of alternative social media applications as major SMAs tighten their policies on political disinformation campaigns. These applications have the potential to bypass government and private sector led ICT service regulations. They include FireChat, Signal, Xender, and Lantern. Fire Chat in particular is turning to be a popular application in cases of Internet shutdown. It is a peer to peer chat app that does not require Internet connection and works within a radius as enabled by Bluetooth and WI-FI direct. These new media apps have been used most predominantly in organising social protests globally such as in Hong Kong and Myanmar, when governments and service providers have suspended or effected total Internet shutdowns.

The applications are evolving to counter the influence of the more popular apps such as Facebook, Twitter, WhatsApp, and Snapchat, which can be disrupted by Internet shut-downs. The shutdowns are interventions applied

FaNkews

but has slowed on the intervention owing to confusion and dissatisfaction among its users to control information spread and also to counter disinformation around sensitive periods such as electoral cycles or social media protests. As of the begining of 2021, Signal has been positioning itself to counter the likely migration of users from the popular WhatsApp, which is effecting changes to its platform in May 2021 to enable the sharing of personal data that would also be linked to Facebook accounts and thus erode user privacy. It had earlier communicated that it would effect these changes by February 2021 .

Unlike traditional media such as the use of newspapers and television, where ideally facts can be checked, social media is influenced by friendship networks and thus creating possibilities for disinformation. Complicating this space further is the possibility of 'deep fakes' where fake videos of politicians could be created to skew public opinion in a particular direction. While there is a growing awareness and growth of fact checking organisations, fake content can easily be spread on social media platforms.

Governments in different parts of the world engage in Internet shutdowns to safeguard national security. These have been justified on the basis of a need to counter disinformation or neutralise organizing of protests. Examples include the 2020 shutdown of Tigray Region in Ethiopia and the Internet shutdown during general elections in Uganda in January 2021. The new recurring question then is, how do social media users adapt to policy controls on applications and the internet in the wake of political disinformation? What are the implications of these adaptations on national security in Kenya?

Photo Credit: Africa Check

The use and exploitation of virtual private networks (VPNs): The case of TOR

A key adaptation strategy likely to be in use for disinformation campaigns is the virtual private networks. VPNs works by encrypting a user's Internet traffic over a dedicated server and which in part overcomes online Internet censorship. This mode can overcome security surveillance. VPNs only require the setting up of a paid account with a VPN service provider. An added layer of complexity is the option of paying for a VPN service anonymously such as the use of Bitcoin.

Another strategy has been to use a VPN provider that is unlikely to pass on data to security agencies. On the overall, given that data is channeled through a central server, it is not a full guarantee that this data may be confidential. There is a possibility that backdoor access of this data could be channeled to security agencies as the Edward Snowden leaks demonstrated.One of the strategies to overcome infiltration and disruption through VPN networks has been the rapid adoption of Tor, an anonymous web browser that is censorship free. Tor emerged in 2003, and covers Internet traffic with layers of privacy (Eaton, 2015).

Once a user connects over Tor, the identifying information is lost, with data being encrypted and privatised before launching into the web. This stripping of identifying information means the Internet traffic such as its origin, is nearly impossible to track (Hodge, 2020). This software is free to download, counters security agencies surveillance and remains anonymous. The downside to this browser are slow speeds, and the need for continuous updates to circumvent security vulnerabilities (Eaton, 2015).

While VPNs are considered secure means of communication, they remain vulnerable to attacks. VPN traffic can be intercepted and modified through malware. One of the weaknesses is that of username enumeration vulnerability. This is when a username/password responds differently to an invalid username/password. If an attacker finds that the username exists, they can perform an offline hacking to access the password given that the VPN is no longer encrypted. Other vulnerabilities of a VPN network include an unsecured password storage, the lack of account lockout, and poor default configurations (Rahimi & Zargham, 2018).

While governments' globally have the capacity and surveillance tactics to counter the disinformation space through the use of total or partial Internet shutdowns, the uncharted path remains the use of VPNs. Social media activists, citizens and politicians alike may exploit a variety of strategies and continue with their propaganda and disinformation tactics (Eaton, 2015). Internet censorship works in at least three ways: one is through the domain name system (DNS), where a country can intervene in its local servers by deleting a blocked website Internet protocol (IP) address; the other option is port blocking, where a country creates a firewall between its citizens and an online platform, making it inaccessible; the third approach is deep packet inspection, where specific Internet sites and or search words can be blocked (Eaton, 2015).

Globally, governments maintain some form of Internet censorship to keep dissidents at bay. China in particular is a notable world leader in Internet censorship. It uses technology to identify and curtail the organisation of public assemblies and demonstrations while simultaneously using it to gauge public opinion (Jost et al, 2018).

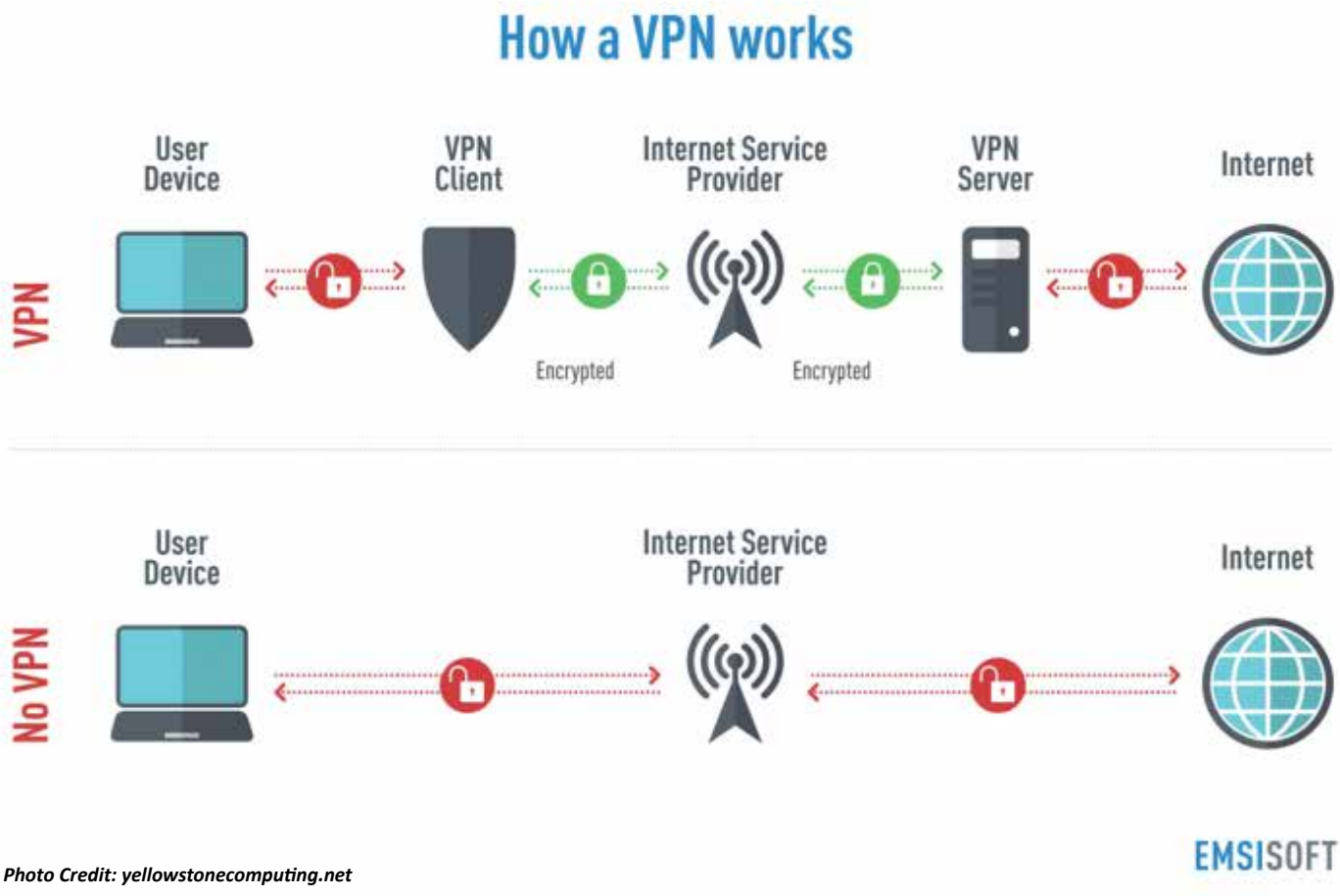

Photo Credit: yellowstonecomputing.net

Silent Penetration of Existing Social Media Applications

Another adaptation strategy in use is the silent penetration of existing social media platforms to evade detection. The Islamic State group (ISIS), a social movement with violent extremist leanings, has rapidly adopted this strategy. This occurs in a context where social media platforms are fast to flag and delete inappropriate content on their platforms.

This strategy is a possible disinformation option ahead of the 2022 electioneering period. ISIS is reported to mix its content with that of real news outlets such as recorded television news, including BBC themed music. It also has the ability to hijack actual Facebook accounts to support its propaganda. This in the past included targeting the walls of public figures such as former US President Trump's Facebook page (Corera, 2020). Another possible disinformation campaign strategy ahead of the 2022 elections that could be applied is breaking up or use of strange punctuation marks to curtail the use of search words. ISIS has perfected the scheme. This could be accompanied by time lags before a disinformation item is flagged and removed. Moreover, social media applications are sometimes reluctant to remove content for its financial gain.

It is further possible that alternative links could be provided even as accounts in mainstream social media are shut. Individuals could be directed to newer social media pages or in encrypted outlets such as Telegram (Corera, 2020). Social media users can further be willing spreaders even when aware the content they are disseminating is fake. This action could be on account that they agree with the views spread (Margolin, 2020). Of interest is the fact that individuals with higher digital literacy rates are likely to spread disinformation (Crest, 2020).

Development of New Social Media Applications

Another possible scenario for disinformation is the possibility of developing new social media applications. These could be further linked to existing applications by way of targeted invitation such as Telegram, Gap, and Parler. As a strategy to circumvent surveillance, opening invite only or other closed groups on social media platforms remains a possibility.

An additional layer of strategy that could be adopted is the constant migration or creation of multiple sites that would include fake accounts to further continue with disinformation.This analysis is not far-fetched. President Trump in the last days of his presidency already hinted at the possibility of creating his own social media platform in response to a ban on his personal Twitter account.This ban came on claims of using his handle to spread disinformation. Additionally, the January 6, 2021 insurrection at the Capitol including future possibilities to incite violence informed the ban. Facebook responded in a similar manner by suspending Trump's account (Rawler, 2021). With a technology savvy population, creation of new media applications for disinformation remains a probable scenario.

Parler, a platform launched in 2018 and largely associated with American right wing users has resurfaced after a month long absence following the January 6, 2021 US Capitol insurrection. This App arose to counter content rules on mainstream media outlets (CNBC, 2021). There are possibilities that new applications outside of the mainstream could become a reality.

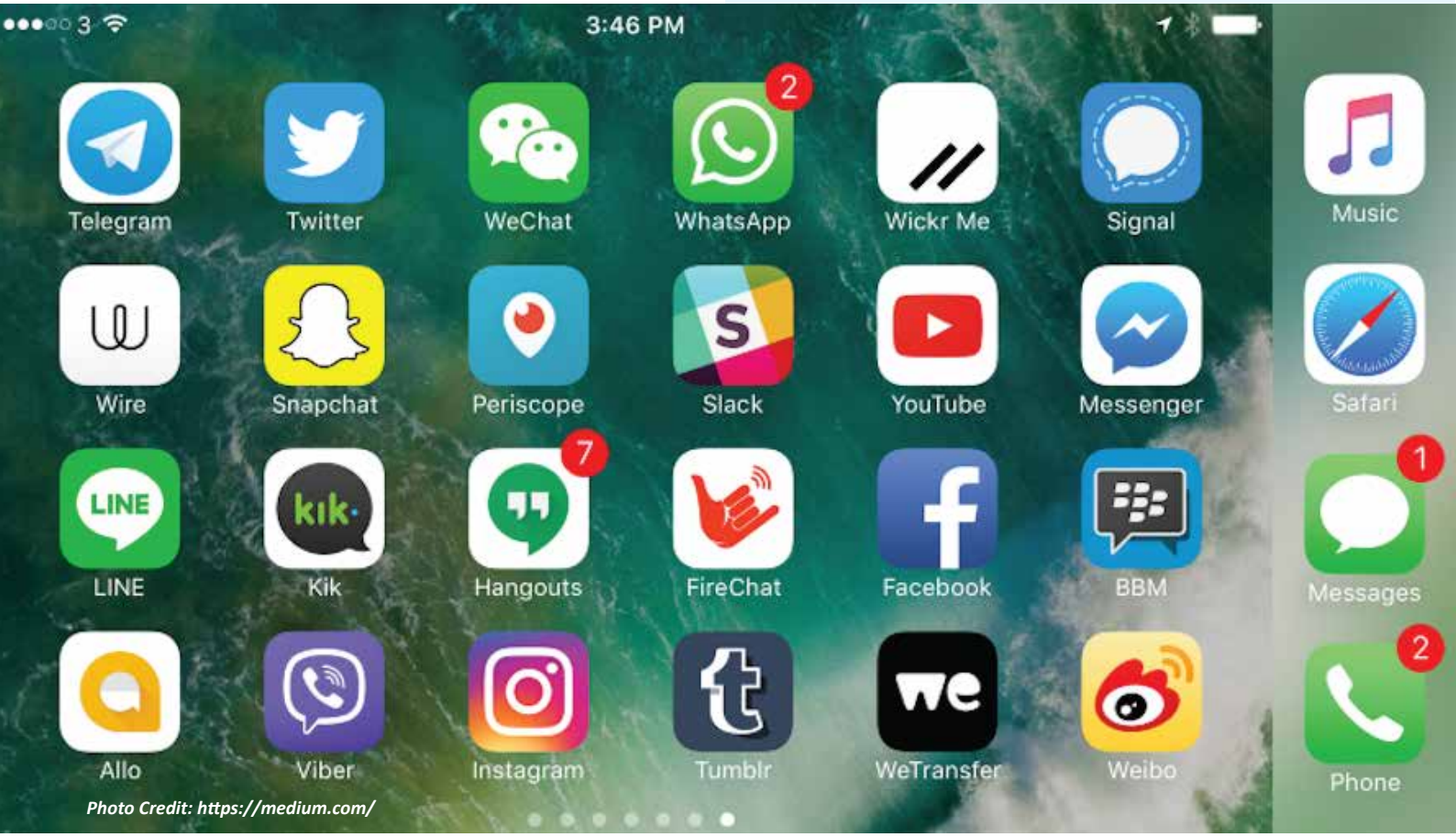

Photo Credit: https://medium.com/

Conclusion

This paper concludes that to minimise the use of disinformation in the run up to 2022 general elections, policy makers have a window of opportunity to tighten legislation, create media literacy, and innovate co-regulation with social media platforms. The paper suggests the creation of a multi-agency social media monitoring unit to counter disinformation and engage in counter-messaging.

Recommendations

a) The National Assembly to fast track Information and Communications Amendment Bill of 2019 to offer more deterrence for the misuse of social media platforms. The current provision of a fine not exceeding two hundred thousand shillings and or a jail term not exceeding one year is less punitive and should be enhanced. There is need for strict enforcement of related legislation such as the Public Security Act (revised 2012), the Data Protection Act of 2019, and relevant provisions of the Penal Code.

b) The Ministry of Interior to create of a multi-agency social media monitoring unit that would be responsible for monitoring disinformation on social media and engagement in counter-messaging. The staffing of this unit would include government-agencies such as the National Intelligence Service (NIS), Kenya Defence Forces, National Police Service, Ministry of ICT, Youth and Innovations. It would be responsible for research, policy recommendations, and mapping patterns and trends on disinformation online.

c) The Ministry of ICT, Innovation & Youth Affairs' should lead an awareness campaign on the negative side of social media applications. Media literacy and critical thinking is an important strategy to create awareness on fake news phenomenon. Civic education, including creating awareness through school systems, could be an additional strategy to sensitise and counter disinformation.

d) The Ministry of Interior to take lead in the development of a voluntary code of conduct for co-regulation between government and social media platforms. This would cover self-regulation guidelines and also be responsive to public interests around disinformation. It will account for social media platforms internal regulatory mechanisms. This is suggested on the basis that legislation is unable to keep abreast of the changing social media landscape. Social media platforms in addition have their own regulatory mechanisms to bring down content that violates policies such as hate speech, fake news, and incitement. Some of the platforms work with fact checking organisations and have prioritised policies to curb fake news in electoral cycles.

References

Anderson, K.E. (2020). Getting acquainted with social networks and apps: it is time to talk about TikTok. Library Hi Tech News 4, 7-12.

BhattaCharjee, S. (2019). FireChat Will be Your Go-To Messaging App When the Internet is blocked https://in.mashable.com/tech/9554/firechat-will-be-your-go-to-messaging-app-when-the-internet-is-blocked (accessed 19th January 2021).

Communications Authority of Kenya (2020). Annual Report 2018-2019. Available at https://ca.go.ke/document/annual-report-for-the-financial-year-2018-2019-2/ (accessed October 22, 2020).

Communications Authority of Kenya and National Cohesion and Integration Commission (2020). 'Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Via Electronic

Communications Networks' (July 2017) <https://ca.go.ke/wp-content/uploads/2018/02/Guidelines -on-Prevention-of -Dissemination-of-Undesirable-Bulk-and-Premium-Rate-Political-Messages-and-Political-Social-Media-Content-Via-Electronic- Networks-1.pdf (accessed October 23, 2020).

CNBC (2021). Social media platform Parler is back online on 'independenttechnology' https://www.cnbc.com/2021/02/15/social-media-platform-parler-back-online-after-being-banned-by-major-tech-companies.html

CREST (2020). Why Do People Share Disinformation on Social Media? https://crestresearch.ac.uk/resources/disinformation-on-social-media.

Corera, G. (2020). ISIS 'still evading detection on Facebook', report says: https://www.bbc.com/news/technology-53389657

Margolin, S. (2020). Why Are Social Media Platforms Still So Bad at CombatingMisinformation?https://insight.kellogg.northwestern.edu/article/social-media-platforms-combating-misinformation

Eaton, D. (2015). Scaling the firewall: Ways around government censorship online https://www.csmonitor.com/World/-Pass code/2015/0420/Scaling-the-firewall-Ways-around-government-censorship-online (accessed 18th January 2021).

Fagan, F. (2018). Systemic Social Media Regulation. Duke Law & Technology Review, 16 (1), 393-439. (2018).

Hodge, R. (2020). What is Tor? Your guide to using the private browser https://www.cnet.com/how-to/ what-is-tor -your-guide-to-using-the-private-browser/ (accessed 18 January 2021).

Jost, J. et al (2018). How Social Media Facilitates Political Protest: Information, Motivation, and Social Networks. Advances in Political Psychology, 39(1), doi: 10.1111/pops.12478

Levush, R. (2020). Government Responses to Disinformation on Social Media Platforms: Comparative Summary. https://www.loc.gov/law/help/social-media-disinformation/compsum.php

Li, S.P. (2021). Facebook was the internet in Myanmar. What happens now that it's banned? https://kr-asia.com/facebook-was-the-internet-in-myanmar-what-happens-now-that-its-banned-tech-in-culture

Martin-Rozumiłowicz, B., & Kužel, R. (2019). Social Media, Disinformation and Electoral Integrity: IFES Working Paper.https://www.ifes.org/sites/default/files/ifes_workinpaper_social_media_ disinformation_and_electoral_integrity_august_2019.pdf

Maweu, J.M. (2019). "Fake Elections"? Cyber Propaganda, Disinformation and the 2017 General Elections in Kenya. African Journalism Studies, 40(4), 62-76, DOI: 10.1080/23743670.2020.1719858

Montgomery, M. (2020). Disinformation as A Wicked Problem: Why We Need Co-Regulatory Frameworks. Accessed 27 October 2020 at https://www.brookings.edu/wpcontent/uploads/2020/08/Montgomery_Disinformation- Regulation_PDF.pdf

Morgan, S. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy. Journal of Cyber Policy,3(1), 39-43, DOI: 10.1080/23738871.2018.1462395

Mutahi, P. & Kimari, B. (2020) Fake News and the 2017 Kenyan Elections, Communication, DOI: 10.1080/ 02500167. 2020.1723662

Norwood, C. (2021). https://www.pbs.org/newshour/politics/how-was-a-violent-mob-able-to- breach-the-u-s-capitol-activists-see-double-standard-in-police-response (accessed 19th January 2021).

Rawler, J. (2021). Donald Trump has been kicked off of Twitter https://www.engadget.com/trump-banned-from-twitter-again-024724093.html

Rahimi, S., & Zargham, M. (2018). Quantitative Evaluation of Virtual Private Networks and its Implications for Communication Security in Industrial Protocols. Journal of Advance Computational Research, 3(1), 51-61.

Republic of Kenya. (2019). Kenya Information and Communication Act (Amendment Bill) 2019. Government Printer.

Republic of Kenya. (2019). Computer Misuse and Cybercrimes Act, No 5 of 2018. Government Printer.

Samples, J. (2019). 'Why the Government Should Not Regulate Content Moderation of Social Media' (Cato Institute, Policy Analysis No. 865, 9 April

2019)<https://www.cato.org/publications/policy-analysis/why-government-should-not-regulate-content-moderation-social - media> accessed 27 October 2020.

Shu, K, Bhattacharjee, A, Alatawi, F, et al. (2020). Combating disinformation in a social media age. WIREs Data Mining and Knowledge Discovery https://doi.org/10.1002/widm.1385

Vasu, N. et.al (2018). Fake news: national security in the post-truth era. Policy Report: Nanyang Technological University, Singapore.