Election Management and Artificial Intelligence in Cameroon

Saron MessembeObia

(An Author and Expert in International Security and Terrorism, and IREX Artificial Intelligence Expert (IREX AI- U.S). A certified Cyber Criminologist, Forensic Expert and Certified Public Policy Analyst at the Nkafu Policy Institute, Yaoundé-Cameroon. He is a researcher for the Research Institute for European and American Studies (RIEAS), Counter Terrorism Analyst at the Islamic Theology for Counter Terrorism (ITCT-UK) and Cyber Security instructor at Wilses Cyber Security Solutions-Zambia, CyberDefenz, Yaoundé-Cameroon and ASID-Academy of International Law, Buea-Cameroon. He served as Assistant Editor and Country Representative for Publication Division at the International Association for Counter Terrorism and Security Professional South East Asia (IACSP SEA), Research at the Cyber Physical System Virtual Organization- Washington DC and is also an Intelligence Analyst. He has authored several articles on cyber security, counter terrorism, stadia security, money laundering and jihadists tendencies in Sub Saharan Africa and Europe, as well as books; 'The Criminal Mind In The Age Of Globalization', 'Cybercrime And AI State, Money, And Power' and Weaponized Drones Terrorism in Africa Al Qeada, Al Shabaab, Boko Haram & ISIS')

Gabriel Cyrille Nguijoi

(Researcher at the National Institute of Cartography (NIC); Research Associate at the African Centre for the Study of the United States, Johannesburg; a lecturer at the Cameroonian Institute of Diplomatic and Strategic Studies (ICEDIS); and a member of the European Centre for the Study of Populism (ECSP), Belgium. He is a PhD graduate from the University of Yaoundé II, that focused on intelligence cooperation against transnational threats in Africa, with a case study on the Lake Chad Basin. He specializes in international relations, security studies, terrorism, para-terrorism, Security Sector Reforms Governance, and socio-spatial dynamics, particularly in Africa. Gabriel's interdisciplinary research explores security challenges, regional cooperation, and the role of geopolitics in shaping conflict and insecurities in the international scene. He has published widely in leading journals.)

Publication date: 24 May 2025

The globalization era has redefined the security paradigm around the world. From internet of things (IoT) to cybercrime and artificial intelligence (AI), which is the theme of discourse at national and international sphere. In order to have a clear bearing of the discourse, it is necessary to highlight some major threats in relation to election management, which will provide insight for policy advocates for fair and transparent elections. One of the major menace to election management is cyber criminality: The Hacking of the Cameroon Presidential Website 2015, thereby uploading a fabricated photo on the website of the Head of State honoring some gallant soldiers killed by Boko Haram appeal on how secured is the cyberspace of the country[1]. The most thrilling case is that of Elections Cameroon (ELECAM) in 2020. The hacking of ELECAM which was attributed to opposition, based on the message and photo posted by the hacker appealing for electoral hold up in Cameroon. All of these breach appeals for proper security policy, measures, and cooperation, in order to better secure the election management database from cyber-attacks, for free and fair elections results.

Keywords: Artificial Intelligence, Cybercriminality, Hacking, Election Management

Introduction

The Cameroon electoral process is a blueprint of that in the western world, following the introduction of biometric registration and other legal principle. Though some fellows tend to criticize the electoral process and management, as of the 2018 elections. The incorporation of artificial intelligence (AI) in the electoral process by its governing body is highly appreciated by Cameroonians. According to ***article 3 paragraph 1 of the 2021 proposal for a European Union (EU) Regulation, also known as EU AI Act*** states that the term ***AI system ''means software that is developed with one or more [...] techniques [...] and can, for a given set of human-defined objectives, generate outputs, such as content, predictions, recommendations, or decisions influencing the environments they interact with'' (Blauth, T. F., Gstrein, O. J., & Zwitter, A. 2022)***. However, the menace of non-conventional crimes is another discourse by civil society, human rights defenders, opposition political parties, and non-governmental organizations on conducting free and fair elections over a decade, and the respect of democratic principles.

Most opposition leaders and civil society activists belief that the process has several irregularities. However, the political landscape in Cameroon ahead of the 2025 presidential elections seems to be accommodating the use of AI, particularly the biometric registration and

[1] http://www.edennewspaper.net/cyber-criminals-hack-presidential-website/

the update version of the electoral list. Notwithstanding, is necessary to have an insight of some of the cases and menace to free and fair elections, which emanate from cybercriminality and hacking in particular. According to ***Law No 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon***: ***Cybercriminality is defined as an infraction of the law carried out through cyberspace using means other than those habitually used to commit conventional crimes.*** A hacker is an individual with IT knowledge, who breach systems or networks, either for financial motive, to obtain intelligence and to showcase his or her talent. However, most of the causes of hacking in contemporary events are link to data collection and financial motives (ransomware) and destructive narrative (cyber-espionage, cyber-attacks and cyber warfare).

Cameroon is one of the main countries who respect regional and continental norms and protocols. At the continental level, leaders, intellectuals, civil society activists and election managers have reflected on the conduct of elections on the continent with the help of independent organizations. An example, is the ***38th Ordinary Session of the Organization of African Unity (OAU or AU) held in Durban, South Africa, on 28 July 2002.*** African leaders subscribed to the Declaration on the Principles Governing Democratic Elections in Africa, which are but not limited to:

a) freely and fairly;

b) under democratic constitutions and in compliance with supportive legal instruments;

c) under a system of separation of powers that ensures, in particular, the independence of the judiciary;

Some scholars and electoral management staff reviewed these principles develop at meeting held in Mauritius, in which statesmen of the Southern African Development Community (SADC) committed themselves to a regional version of the AU Declaration by adopting the Principles and Guidelines Governing Democratic Elections. Other fellows benchmark on key issues which could be useful to the Cameroon government. Some of the key issues are, but not limited to:

- The establishment of appropriate institutions to address thorny issues relating to election management, such as codes of conduct, citizenship, residency, age requirements and other voter/candidate eligibility conditions.

- The establishment of impartial, all-inclusive, competent and accountable national election management bodies staffed by qualified personnel.
- The establishment of relevant courts to arbitrate electoral disputes.
- The prevention and repression of electoral fraud.

Drawing from these principles outlined above, Cameroon is gradually closing the gap regarding election management. However, biometric process and electoral management and proclamation of result will be of interest in the next elections in Cameroon.

In order to comprehend election management and artificial intelligence in Cameroon, is necessary to have a brief background of the democratic process. From 1990s multi party politics dynamics in Cameroon through protest in Yaounde. As of now Cameroon has more than 200 authorized political parties. Opposition political parties press for political reform, particularly the setting up of an Independent Electoral Commission (IEC).

On the 19th December 2000, a law was enacted to set up a National Elections Observatory (NEO), whose duty is to supervise and control all elections and referendums organised in the country. ***The creation of ELECAM in 2006 as per law No 2006/011 0f 29 December 2006 which setup and lay down the organization and functioning of Elections Cameroon (ELECAM)***, change the dynamics of the electoral process with the use of AI and other related tools.

Election Management and AI: Problems and Prospects

One of the major challenges of election management is public confidence in the electoral process, during the proclamation of result. The proclamation of result usually initiate contention between opposition political parties and the ruling party. For example, the administrative litigation with opposition parties in 2018, which some citizens were apprehended for violating certain legal principles.

Menace pose by artificial intelligence during elections: review of some cases

Hacking of the Presidential Website 2015

The president of the republic has been active for the past month on social media platforms. Meanwhile, according to an ***ANTIC audit, 27,052 vulnerabilities were detected in public and private administrations' IT systems in 2021***.

More so, the hacking of the presidential website on March 2015, a fabricated photo of the Head of State being uploaded on the website (while he was on vacation in Europe) honoring some gallant soldiers murder by Boko Haram pose a strategic problem on how secured is Cameroon's cyberspace. Whereas, on 6 March 2015, the president of the republic was represented by the Minister Delegate at the Presidency in charge of Defense[2].

Hacking of Elections Cameroon (ELECAM) 2020

The hacking of ELECAM would have been allegedly linked to opposition party, view the message and photo posted by the hacker (correlating to the message of an electoral hold up in Cameroon)[3]. This incident reveals the vulnerability of the cyberspace, as ***ANTIC claims it deleted 3,372 fake Facebook accounts out of 4,242 identified in 2020***.

Though the president of the electoral board of Elections Cameroon, Enow Abrams Egbe reacted officially to the situation, in a communique signed June 24, 2020, and place a red notice to track down the criminals who engage in this act. It is necessary to understand that the world have taken a new shift with artificial intelligence, the question is how can the attacks be countered or mitigated.

However, on august 2020, two suspects were apprehended after investigations of experts in cybercrime from the National Agency of Information and Communication Technologies (ANTIC), who criticized the use of "anti-patriotic words".

Moreover, some opposition politicians and civil society actors are critical about the electoral code, don't trust of workers of the organization, question the manner in which these personalities are recruited, and the efficiency in election management duties. Nevertheless, of the numerous entities which have been responsible for various election management tasks, ELECAM seem to be credible to some fellows due to the implementation of biometric registration, accuracy in the management of data ahead of the 2025 presidential elections. ELECAM has breach the odds, by meeting Cameroonians even in hinterland areas for the registration on the voters list.

The emergence of artificial intelligence and other new technologies facilitates election management. The adoption AI for election management tasks such as the establishment of electronic voters' rolls and cards, election results and statistics are very vital to the government. However, the hacking of ELECAM post 2018 presidential elections expose the

[2] http://www.edennewspaper.net/cyber-criminals-hack-presidential-website/
[3] https://newsupfront.com/elections-cameroons-hacked-account-kamto-reacts-elecam-threatens/

menace on the electoral process in Cameroon. Though, there is no specific legislation on artificial intelligence (AI) in Cameroon the existing data protection law (***Law No 2024/017 of 3 December 2024 relation to Personal Data Protection in Cameroon***) is a guide for a future AI law.

Conclusion

The 2018 presidential election in Cameroon provide new insight on amendments to be made and the need for adequate security measures to avoid future menace, like the hacking of electoral board, the litigation opposing the ruling party and opposition party. According to Thaddeus Menang in reflection to Matlosa…democracy cannot simply be imported into a country as one would import a car. But whether or not social democracy is a truly viable option remains to be seen...In as much as, the Cameroon government has created institutions such as: ***Ministry of Post and Telecommunication*** which is charge of electronic communications and consumer protection in Cameroon; Agency's like ***ART*** is the regulator of the mobile and operating; ***The National Agency for Information and Communication Technologies (ANTIC)*** is in charge for the ICT sector in Cameroon communication networks, other security agencies must engage experts in order to help draft policy.

Cameroon government needs to ensure and make use of cyber security experts to counter any attack on the ELECAM website and to secure biometric data collected, from voters before and after elections. It is necessary for the election management board to also cooperate with resource persons to draft policy and review and develop recommendations after elections, despite the involvement international observers for a free, fair and transparent election in Cameroon.

References:

Atsa, E 2016. Development of The Digital Economy in Cameroon: Challenges and Perspectives, in The Electronic Journal of Information Systems in Developing Countries, EJISDC (2016) 76, 7, 1-24

Cekerevac, Z. et al. Hacking, Protection And The Consequences Of Hacking. Komunikacie · June 2018

China's AI Regulations and How They Get Made by Matt Sheehan. HORIZONS Summer 2023, No.24

Duflot, A. 2024. Artificial Intelligence in the French Law of 2024. Legal Issues in the Digital Age. 2024. Vol. 5. No. 1.

Eric Akuta E , Ong'oa M and Chanika R.J ''Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice'' Journal of Research in Peace, Gender and Development Vol. 1(4) (2011) at 113

LATHAM & WATKINS. China's New AI Regulations. August 16, 2023 | Number 3110

Marcin Szczepański 2024 United States approach to artificial intelligence. European Parliamentary Research Service

Mozaffar, S. 2002. 'Patterns of Electoral Governance in Africa's Emerging Democracies'. International Political Science Review 23(1).

Matlosa, Khabele. 2003. 'Electoral Systems and Multiparty Democracy in Southern Africa'. Paper presented at the Conference on Elections, Democracy and Governance, Pretoria, South Africa, April.

Olivier Nana, O and Tankeu, R 2012 Understanding what is happening in ICT in Cameroon; A supply- and demandside analysis of the ICT sector, in Evidence for ICT Policy Action Policy Paper 2, 2012

Patricia Asongwe (2019). The Principle of Legality of Crimes and Punishment Migrates to Cyberspace: An Appraisal of the Cameroonian Experience. South Asian Law Review Journal. Volume 5 -2019

SADC Parliamentary Forum. 2001. 'Norms and Standards for Elections in the SADC Region'.

Thaddeus M. 2006. Election Management in Cameroon. Progress, Problems and Prospects. Journal of African Elections. Volume 5 No 1

https://www.businessincameroon.com/public-management/0703-12393-cameroon-lost-xaf12-2-bln-to-cybercrime-in-2021-antic

https://www.businessincameroon.com/public-management/2106-11696-cybersecurity-antic-claims-it-deleted-3-372-fake-facebook-accounts-out-of-4-242-identified-in-2020

https://www.cameroun.cc/cyber-criminality-law-in-cameroon/

https://www.cameroon-tribune.cm/article.html/34722/fr.html/lutte-contre-la-cybercriminalite-les-entreprises-en-premiere-ligne

https://www.cameroon-tribune.cm/article.html/34722/fr.html/lutte-contre-la-cybercriminalite-les-entreprises-en-premiere-ligne

https://enixcompany.com/blog/actualite-5/post/cameroun-et-cybersecurite-4

https://www.digitalbusiness.africa/cybercriminalite-des-pertes-annuelles-au-cameroun-en-milliards-de-f-cfa/