Research Paper

No. 191

May 2026

E-CRIMES AND AI:

Rethinking Data Privacy and National Security in Cameroon and Kenya

Saron Obia Messembe[1] & Aigbe Diyeli Segun (PhD)[2]

ISSN: 2241-6358

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

 # 1, Kalavryton Street, Alimos, Athens, 17456, Greece

RIEAS: http://www.rieas.gr

[1] *Consultant at Ground Truth Intelligence, Executive Director Intelligence Security Solutions, Researcher at Research Institute for European and American Studies (RIEAS), Theorist Coordinator at Cyber Jurisprudence International Initiative (Egypt), Public Policy Analyst at Nkafu Policy Institute (Cameroon), sirmessembe@gmail.com*

[2] *Department of Criminology and Security Studies, Caleb University, Imota, Lagos State-Nigeria. Diyeli.aigbe@calebuniversity.edu.ng & aigbediyeli@gmail.com*

RIEAS MISSION STATEMENT

Objective

The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

Activities

The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

Status

The Research Institute for European and American Studies is a non-profit research institute established under Greek law. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

Prof John M. Nomikos
Director

Research Associates

Panagiotis Kollias (BA), Transatlantic Security Studies
Matan Uberman (MA), International Security Studies
Robbin Griffith, Central and Eastern Europe Studies
Marina Artemeva, Northern Caucasus Studies
William Tucker, U.S. National Security Studies
Prem Mahadevan (PhD), Indian Counter Intelligence Studies
Christodoulos Ioannou (MA), European Intelligence Studies
Nikolas Stylianou (MA), Cyprus and European Studies
Konstantinos Saragkas, (MSc , LSE), ESDP/European Armaments Cooperation
Nickolaos Mavromates (MA), Greek-Israeli Relations

Research Paper
No. 191
May 2026

F-CRIMES AND AI:

Rethinking Data Privacy and National Security in Cameroon and Kenya

Saron Obia Messembe[3] & Aigbe Diyeli Segun (PhD)[4]

ISSN: 2241-6358

Abstract

Data privacy is essential for national security and state sovereignty. With the emergence of non-conventional crimes with the use of artificial intelligence, no one is safe. Following the hacking of Nigeria secret service database on August 2012[5], to election management in Kenya and Cameroon, not isolating presidential websites hacking, are evidence to appeal for new security strategies and policy line to secure the Africa's cyberspace. In as much as, cyber laws have been enacted, understanding the modus operandi of these criminals, application of these laws are

[3] ***Consultant at Ground Truth Intelligence, Executive Director Intelligence Security Solutions, Researcher at Research Institute for European and American Studies (RIEAS), Theorist Coordinator at Cyber Jurisprudence International Initiative (Egypt), Public Policy Analyst at Nkafu Policy Institute (Cameroon), sirmessembe@gmail.com***
[4] ***Department of Criminology and Security Studies, Caleb University, Imota, Lagos State-Nigeria. Diyeli.aigbe@calebuniversity.edu.ng & aigbediyeli@gmail.com***
[5] Is cyberspace the latest conflict frontier on the African Continent Published. February 28,2017 by THE CONERSATION

sometimes challenging, due to inadequate expertise and the technicality of the 'game'. This paper does not only expose the different cybercriminal cases in Cameroon and Kenya, it also appeals for collaboration with experts in the domain to better secure, mitigate and help in policing these crimes. The question now is why election management and hacking of presidential websites? Cyber-attack on election management system and presidential websites prior to the publication of results can spark insecurity in a nation. AI has increase the vulnerability of some African countries, even with the installation of security software for system management. Defacement of presidential websites and the uploading Deepfake videos can propagate hatred and insurrection due to the proliferation these applications. This paper appeals for synergy amongst actors like penetration testers, ethical hackers, software engineers and cyber bug-bounty experts to help secure systems prior and post elections for peace and sustainable development in Africa.

Keywords- Cybercrime, Ransomware, Hacking, Artificial Intelligence, African Union

Justice is driven by science not speculation[6]. Several African countries have been victims of ransomware attacks for more than a decade. Criminals always target public infrastructures; hospitals, financial entities, internet service providers and international organizations. The African Union (AU) has been a target of the **BlackCat Group** (also known as ALPHV) particularly on her internet connectivity in 2023, the international criminal police (Interpol) and partners[7] responded to the incident and further secured the system.

[6] Adage drawn from a speaker at the 1st Forensic International Conference organized by The Forensic Post on 22nd to 23rd of February 2025

[7] Le Monde (2023) : https://www.lemonde.fr/afrique/article/2023/04/25/vent-de-panique-a-l-union-africaine-apres-une-nouvellecyberattaque_6170976_3212.html

Cameroon and Kenya have promulgated several laws to combat the emerging menace of cybercriminality, which is becoming a national security challenge. While Kenyan criminal justice system exploit ***The Computer Misuse and Cybercrimes Act, 2018 and The Data Protection Act, 2019 (No. 24 of 2019),*** Cameroon is changing the narrative with; ***Law N° 2010/012 Of 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon; Law No 2010/021 0f 21 December 2010 on Electronic Commerce in Cameroon; Decree No. 2015/3759 of 3 September 2015 Lay Down the Identification Requirments for Subscribers and Terminal Equipement of Electronic Communication Networks; Decree No 2017/2580/PM of 06 April 2017 Setting the Terms and Conditions for the Establishment or Operation of Electronic Communication Networks and Supplies of Electronic communication Services subject to the Authorisation Regime; and Law No 2024/017 of 3 December 2024 relation to Personal Data Protection in Cameroon***. In order to better understand the dynamics of cybercriminality and cybersecurity with the use of artificial intelligence in Cameroon and Kenya, several cases need to be reviewed, to provide insight of the modus operandi and new tech tools available in the dark market exploited by criminals.

Artificial intelligence (AI) is the capability of computer systems to mimic task typically associated with human intelligence, such as learning, reasoning, resolving problems and making critical decision. One will be fast to say; artificial intelligence (AI) is the new paradigm of internet of things (IoT). However, the positive impact is evident, that of enhancing efficiency and automation; improving decision making; enhancing customer experience; reducing human error and risk, as well as cost reduction. In as much as there is a positive narrative, AI has also

expose some negative aspect; lack of creativity; skill loss in humans; ethical and privacy violation; inaccuracies; deep fakes and other fraudulent activities.

Law N° 2010/012 Of 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon provides concise definition of concepts and terms use in policing non-conventional crimes, which are essential for the elaboration of criminal investigation strategies and understanding the changing patterns of crimes. Some of the definition of concepts and terms to be use are:

Cybercriminality: infraction of the law carried out through cyberspace using means other than those habitually used to commit conventional crimes.

Cybersecurity: technical, organizational, legal, financial, human, procedural measures for prevention and deterrence and other actions carried out to attain set security objectives through electronic communication networks and information systems, and to protect privacy.

Data: representation of facts, information or concepts in a form suitable for processing by terminal equipment, including a program allowing it to perform a function;

Connection data: data relating to the access process in an electronic communication;

Traffic data: data relating to an electronic communication indicating the origin, destination, route, time, date, size and duration or type of underlying service.

The Cameroonian 2010/012 law provides a clear distinguish between connection data and traffic data. The state also developed laws relating to technological equipment, such as: ***No. 2015/3759 of 3 September 2015 Lay Down the***

Identification Requirments for Subscribers and Terminal Equipement of Electronic Communication Networks; Decree No 2017/2580/PM of 06 April 2017 Setting the Terms and Conditions for the Establishment or Operation of Electronic Communication Networks and Supplies of Electronic Communication Services subject to the Authorisation Regime. What is ransomware? How does AI facilitate ransomware attacks?

Ransomware is a malicious software design by cybercriminals and deploy to infiltrate networks, take down systems, and encrypt data of victims. Ransomware are usually use to steal confidential information, which the criminal threatens to leak to the public, unless a ransom is paid. Strategies to mitigate ransomware attacks have never been efficient and funds requested is usually high as the crime is being committed with sophisticated tools.

Barracuda's 2023 recent market report on ransomware insights, found that almost three-quarters (73%) of respondents were hit with a successful ransomware attack in 2022, and 38% were hit more than once[8]. Cybercriminals exploit AI to develop sophisticated ransomware attacks. More so, AI and automation is used to craft phishing, vishing (voice phishing over the telephone), and smishing (SMS-based phishing) messages. Network attack application are optimized with data exfiltration.

Enabling ransomware attacks is a menace to states. For instance, the recent ***ransomware attack on the Cameroon National Social Insurance Fund (CNPS) in 2024***. The attack on Cameroon CNPS incurred negative impact on 1.5 million

[8] This changes everything: Ransomware in the age of AI by Barracuda.
https://assets.barracuda.com/assets/docs/dms/ebook-ransomware-in-the-age-of-ai-uk.pdf

citizens data compromised and hacker (s) requesting for ransom after exposing the attack on the Darkweb and appealing to sale the information[9].

This paper shall focus on the legal and ethical implications of the cyber laws in the two African nations. Some of the cases which shall be discuss will focus on, but will not be limited to: data protection and privacy, cybercrime, hacking and ransomware attacks.

Election management in Kenya in 2013

During the 2013 elections in Kenya, a significant number of polling stations saw the kits procured for both Electronic Voter Identification and Results Transmission failing due to inadequate power supply. According to Privacy International (2024) statistics of 2013 elections, only 23% of Kenya had electricity[10], and the school buildings being used as polling stations generally were not equipped with power outlets, with practical evidence in rural areas. Privacy International (2024) further revealed that, most laptops being used for biometric registration of voters had battery issues, and the unavailability of power supply, prompted clerks to resort to the printed register for manual verification of voters[11].

Moreover, the exploitation of mobile phones to transfer tallies of provisional results for centralized calculation was inaccessible due to forgotten PINs, low battery, and data connectivity problems[12], with poll workers being airlifted by helicopter to Kenya's capital, Nairobi, to deliver results manually. With regards to

[9] Digital transformation without safeguards: The CNPS data breach and its lessons for Cameroon. https://paradigmhq.org/digital-transformation-without-safeguards-the-cnps-data-breach-and-its-lessons-for-cameroon/

[10] https://www.npr.org/sections/alltechconsidered/2013/03/09/173905754/how-kenyas-high-techvoting-nearly-lost-the-election

[11] Privacy International (2024) Election Technology in Kenya A tech explainer

[12] https://www.aljazeera.com/opinions/2013/3/29/technology-transparency-and-the-kenyangeneral-election-of-2013

the different challenges, the IEBC's centralised tallying servers overloaded and crashed[13] after processing only 17,000 of the 33,000 polling station results[14] appealing IEBC to suspend the announcement of provisional results, having to wait for the physical FORM 32As to be brought to Nairobi.

Furthermore, a "computer bug" altered the pattern of the election management system, thereby counting each rejected ballot 8 times[15] in the initial tally – which prompt an inflating number of rejected ballots to more than 330,000 instead of the correct figure of circa 41,500. After the proclamation of opposition leader Uhuru Kenyatta as the winner, with 50.07% , a minuscule majority of just 8,000[16] out of 12 million ballots cast. However, losing incumbent Raila Odinga petitioned Kenya's Supreme Court[17] for election malpractice and for the nullification of the official results, appealing the recount of ballots at 22 polling stations. Uhuru Kenyatta was endorsed as the President Elect of Kenya[18] even after the recount appeal by Ralia Odinga.

Data protection and preservation is essential to states, as such, the electronic tools procured for the 2013 election were ultimately put into storage, though 125 of the Electronic Voter ID kits were stolen[19]. According to the electoral commission, these stolen devices only contained raw registration data which had not been

[13] https://www.ft.com/content/c69cb0da-8679-11e2-ad73-00144feabdc0
[14] https://icj-kenya.org/wp-content/uploads/2023/01/ELECTION-TECHNOLOGY-AND-ELECTORALJUSTICE-IN-KENYA-Final-1.pdf
[15] https://www.bbc.co.uk/news/world-africa-21707152
[16] https://www.washingtonpost.com/world/africa/kenyatta-wins-kenya-presidential-election-bynarrow-margin/2013/03/09/c07ae7fa-88b1-11e2-9d71-f0feafdd1394_story.html
[17] https://www.bbc.co.uk/news/world-africa-21812559
[18] https://www.dw.com/en/kenyan-court-upholds-kenyatta-election-odinga-concedes/a-16710263
[19]https://www.standardmedia.co.ke/article/2000073374/kenya-iebc-misses-target-by-four-millionvoters

processed for inclusion in the register of voters, and that any data stored on the devices is encrypted at rest[20].

Hacking of Elections Cameroon (ELECAM) Facebook page 2020

The term hacker is criminalized in most African countries. However, the definition and categorization of the term is essential in criminal investigations. A hacker is someone with IT knowledge, who breach systems or networks, in order to expose talent, for financial reasons and for security intelligence. Some of the core traits of hackers are but not limited to; patience; must be organize and good planner, in order to gain access to networks, social and business platforms after checking vulnerability with the use of ***Shodan***.

There exist several types of hackers; black-hat hackers; white-hat hackers and gray-hat hackers. Following the breach of the presidential website in Cameroon, this piece shall focus on the role of black-hat hackers and white-hat hackers to provide inside on policing crimes. The world is at war, and it is fought on the cyberspace with the use of state-sponsored hackers, reasons why is necessary to know the causes of hacking: hacking to collect data; financial reasons; destructive narrative and hacking for fun.

The San Bernardino case in the U.S change the narrative about hackers in security milieu across the world. When the ***Federal Bureau of Investigation (FBI)*** requested Apple company to unlock a device used by a suspected criminal and the latter denied, invoking the right to privacy and the bureau had to hire an external ethical hacker to unlock the device.

[20] https://www.citizen.digital/news/stolen-laptops-bvr-kits-were-not-used-in-2017-2022-electionsiebc-n316222

The hacking of ***Election Cameroon Facebook page in 2020*** spark a lot of controversy on how secured is the country's cyberspace. The incident which was initially attributed to opposition affiliates, based on the message and photo posted by the hacker, appealing for an electoral hold-up in Cameroon. The President of the electoral board of Elections Cameroon, Enow Abrams Egbe reacted to the incident, in an official communique signed on June 24, 2020, and placed a red notice to track down the criminals engaged in the act[21].

On August 2020, two men, 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". They were further detained at the judicial police headquarters in Yaoundé for over four days. The two suspects confessed to have hacked the Facebook page of Elections Cameroon (ELECAM) on June 23, 2020[22]. Hacking is an emerging menace which needs serious attention and the involvement of strategic actors like; cyber criminologist, penetration testers, cyber bug-bounty experts, forensic experts and ethical hackers in order to redefine Cameroon's cybersecurity landscape.

Hacking of Cameroon's Presidential Website in 2015

According to ANTIC (2014) Cameroon is still at the infant stage with digital technology, (manual to digital) records, show that about 84% of Cameroon government agencies use the internet, 13% under construction, and 3% without the internet. In 2014, Internet coverage of Cameroons' national territory was 80% and the rate of penetration of networks according to the National Agency for Information and Communication Technologies (ANTIC) was 50%.

[21] https://media.neliti.com/media/publications/545919-terrorism-and-technology-246399d3.pdf
[22] 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

In 2015, ANTIC revealed that: regional banks lost at least CFA 3 billion (more than US$5 million) through deeds of skimming, local telephone companies CFA 18 billion and the state CFA 4 billion. The statistics above reveals the menace and vulnerability of Cameroon's cyberspace.

However, some scholars tend to believe that: ***'The law protects the criminal than the citizen'***. The vulnerability rate of software used in Cameroon, explains the emergence of non-conventional crimes, such as: social engineering or cyber-attacks, website defacement and hacking. On March 2015, a fabricated photo of the head of state, chief of arm forces was uploaded on the website of the presidency (while the latter was on vacation in Europe) honoring some gallant soldiers killed by Boko Haram.

Source: Eden Newspaper

Whereas, on 6 March 2015, the president was represented by the Minister Delegate at the Presidency in charge of Defense. The then Minister Delegate at the Presidency in charge of Defense decorated the soldiers posthumously with different ranks. However, the fabricated photo uploaded on the presidential website

days after was that of the president of the republic instead of the minister delegate at the presidency in charge of defense. The photo created so much controversy with local newspapers, bloggers, and politicians rebuking administrative response.

In 2016, ANTIC revealed that, at least 20 government establishments including the National Assembly and the Cameroon Radio Television had fallen prey. The director further added that, about 90 percent of applications and operating systems Software used in Cameroon have been hacked. However, Cameroon is gradually changing the narrative in the domain of cybersecurity, not only by promulgating cyber laws, but also educating and empowering her youthful population on how to secure their systems with open source intelligence (OSINT) and proper use of artificial intelligence (AI).

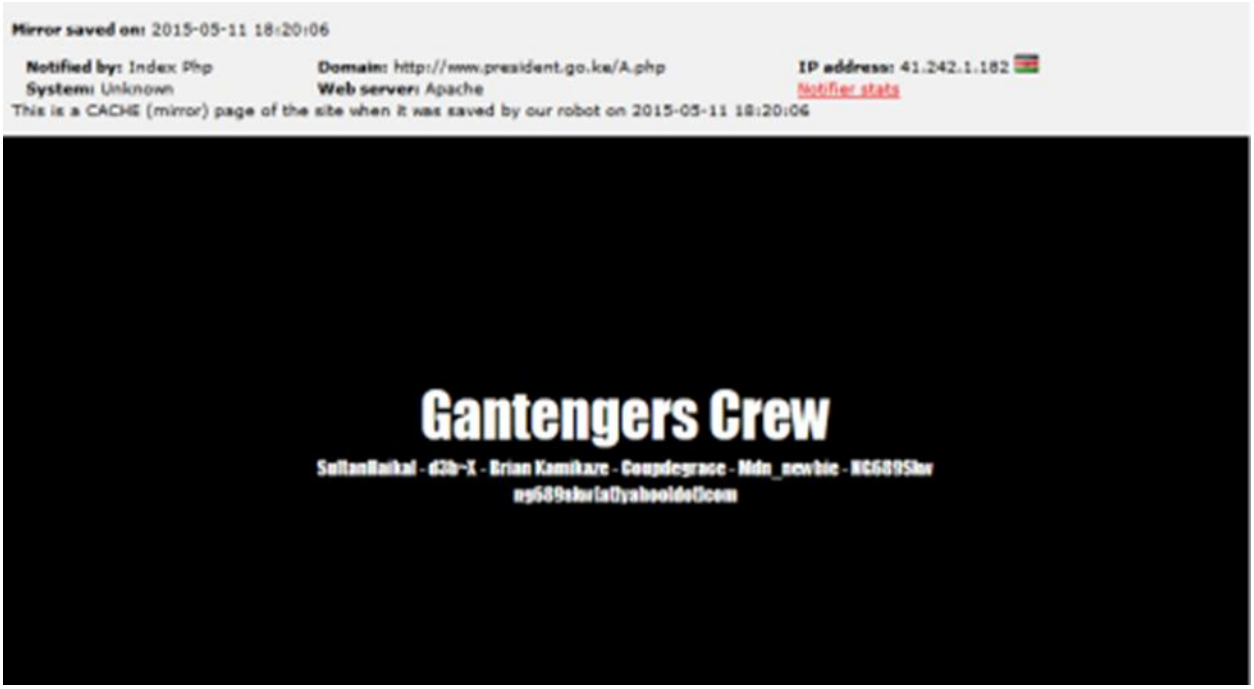
Hacking of the president's website in Kenya 2015

Cybercriminals continue to derive new techniques for social engineering. One of the formidable pattern use by cybercriminals is phishing, which facilitates collection of private information. For example, the ***LinkedIn email scams in 2015 are an illustration of phishing*** (Forbes, 2015). The aim of gaming the system is to collect personal data for instance, an email messages from another person proposing to work at a bank, while requesting for password or keylock. ***The "Business email Compromise" Scams in 2015 and PayPal Phishing Breach in 2016 are good examples (SM, 2015)***. However, is necessary to understand that social engineering, particularly those requesting for money is a strategic pattern for generating personal data such as passwords.

Fayo (2012) cited by Kibe (2018) revealed that in 2012, a Forum Code Security ***"hacker known as direxer, exploited a Web vulnerability and took down 103 government of Kenya websites overnight sitting unfixed programming errors in***

code" a major blow to national security. More so, the available applications like HUNTER.IO and Shodan which are exploited by criminals to check vulnerable networks, servers and CCTV cameras this pose to a strategic menace to national security.

According to LTN (2015) in Kibe (2018), in ***May 2015 some renowned Indonesian hackers from Gantenger's Crew hacked and defaced the President of Kenya's site.*** The defaced webpage revealed the internet handles of the criminals. They replaced the page with one of their own. According to Hack Read reports, the reason behind the targeted site was to reveal to authorities how vulnerable the system is.



Indonesian Hackers Hacked President of Kenya Website [Source: LHN., (2015)] in Kibe (2018)

International and regional cooperation is essential in combatting non-conventional crimes across the African continent. In as much as, the International Criminal Police (Interpol) and the Federal Bureau of Investigation (FBI) usually carry out

raids in African countries to crack down criminals, law enforcement officers need proper training in information and communication technology, particularly in the domain of penetration testing, team of ethical hackers and experts in cyber bug-bounty in order to effectively police these crimes.

The proliferation of AI tools like the ***Flipper Zero***[23] is another strategic menace, added to applications like Shodan which expose vulnerable servers, cctv cameras and other connectivity. Thou there are cyber laws, the inadequate expertise of the policing channel will always lead to acquittals in court, due to lack of evidence or misguided knowledge about the modus operandi, tools and software exploited by these criminals to perpetrate these crimes. Cybersecurity requires resilience, understanding and practical knowledge of the game.

Conclusion

The need to adapt to new technologies in Sub Saharan Africa, is now than ever necessary to validate democratic principles with the emergence of artificial intelligence. Though Cameroon and Kenya are addressing this narrative, as the use of new technologies in electoral process such as biometric voter registration, electronic results transmission systems, and electronic candidate registration management systems presents some challenges, which needs to be reviewed for free and fair elections. Election technology have the potential to improve transparency and foster public trust in the electoral systems. Kenya is an example on how election management technology has reduce violence.

[23] For a basic presentation of the characteristics and specifications see https://www.michigan.gov/msp/-/media/Project/Websites/msp/iod/cyber/CS-01 2025_Flipper_Zero.pdf?rev=2abcff56c1284dfbad4948cd73efae49. Flipper Zero: A Threat to Your Business or a Novelty Gimmick?, 19 February 2025, available at https://www.normcyber.com/blog/flipper-zero-a-threat-to-your-business-or-,a-novelty-gimmick/

More so, the use of this technology is not only essential in mitigating violence during elections, but it also reduces the occurrence of corruption and ballot box stuffing[24], prior to the case of international observers. It is important to accentuate however, the specific circumstances in which the use of election technology could be seen as a possible solution to uphold democracy and avoid corruption.

Corruption is not limited to financial gain, there is intellectual corruption which involves criminal intent, which narrative can affect national security. For example, the breach on the Nigeria Secret Service database reveals the level of vulnerability of some African countries and the need to rethink the security of other agencies, but that of the electoral management board in order to avoid any breach or bug prior to an election.

Though in Cameroon some opposition leaders are critical about the deployment of election technology and lack of transparency. In Kenya, the deployment of election technology initiated trust in the voting process by partially eliminating the potential for human corruption. Moreover, the development of Deepfake is another strategic threat to election management and national security prior and post result publication. With the use of artificial intelligence, controversial videos and documents are easily generated which could spark disputes, amongst parties and even nations. Technological failures have been revealed, which appeal that when rolling out any technology, it is necessary to have manual process in place that is able to replace the automation in case of breach, failure or theft (Privacy International,2024). A world without fact-checkers, is that where AI engineers conflict.

[24] http://kenyalaw.org/caselaw/cases/view/240578/

REFERENCE

Bensamoun A (2018) Stratégie européenne sur l'intelligence artificielle: toujours à la mode éthique. Paris: Dalloz, p 122

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. IEEE Access, 10, 77110-77122. https://doi.org/10.1109/ACCESS.2022.3191790

Goodman J (2016) Robots in law: how AI is transforming legal services London: Ark group, 148 p

Haenlein M , Kaplan A (2019) A brief history of artificial intelligence: the past, present and future of artificial intelligence California Management Review, no 4, pp 5–14

Kibe (2018) An Experiment to Determine the Effect of Ethical Hacking on IT Administrator's Patch and Vulnerability Management Attitudes, a case of a leading telecommunications company. Masters of Science in Information Systems of the School of Computing and Informatics, University of Nairobi.

INTERNET PENETRATION IN CAMEROON. Available from: https://www.statista.com/statistics/640127/cameroon-Internet-penetration/

MINPOSTEL 2017, Major Projects. Available from: https://www.minpostel.gov.cm/index.php/en/lesgrands-chantiers/292-broadband-infrastructure-for-a-digital-cameroon-by-2020, accessed 2017

Republic of Cameroon, The Sector Strategy for Telecommunications and ICT (2005-2015). Available from: https://www.researchictafrica.net/countries/cameroon/Sector_Strategy_for_Telecommunications_and_ICT_2005-2015.pdf

Ahmad, K., JayantShekhar, Kumar, N., Yadav, K.P. 2011. Policy Levels Concerning Database Security; International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044- 6004) 368 Volume 2, Issue 3, page(s); 368-372

Ajzen, I., Fishbein, M. 1980.Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs, N.J.: Prentice-Hall.

BITSIGHT. 2017. A growing risk ignored: Critical updates [Online] Available from https://info.bitsighttech.com/bitsight-insights-a-growing-risk-ignored-critical-updates [Accessed: 16th June 2018]

Bulgurcu B., Cavusoglu H., Benbasat I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly [Online] Available from https://s3.amazonaws.com/academia.edu.documents/30986994/bulgurcucavusoglubenbasat.pdf?

Collier, M., Endler, D. 2014. Hacking Exposed: Unified Communications & VoIP Security Secrets & Solutions. McGraw Hill, New York

EDC., 2018. Cyber Risk Management Has Become Essential to Protecting Business Operations [Online] Available from https://edc.trade/cyber-risk-component-of-enterprise-risk-management/ [Accessed: 2nd November 2018]

Engebretson, P.(2013). The Basics of Hacking and Penetration Testing.Elsevier, USA

Falk, C. (2005) Ethics and hacking: the general and the specific, Norwich University Journal of Information Assurance,1(1).

Fogg B.J. 2003. Persuasive Technology: using computers to change what we think and do, Morgan Kaufmann Publishers, CA

Kharpal, A. 2015. Ethical hacking: Are companies ready? [Online] Available from https://www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html [Accessed: 4th January 2018]

Mforgham S (2010). Cameroon to set Up Cyber Police Force; Africa News.com.http://www.africanews.com/site/Cameroon_to_set_up_cyber_police _force/list_messages

Mforgham S (2010). Cameroon:22 Internet Fraudsters Arrested, Africa News,http://www.africanews.com/site/Cameroon_22_Internet_fraudsters_ arrested/list_messages

Prasad, M., Manjula, B. (2014). Ethical Hacking Tools: A Situational Awareness. Int J. Emerging Tec. Comp. Sc. & Elec.11, 33-38

Right, Tom. 2017. Did unpatched Microsoft exploit lead to massive NHS ransomware attack? [Online] Available from https://www.channelweb.co.uk/crn-uk/news/3010030/did-unpatched microsoft-exploit-lead-to-massive-nhs-ransomware-attack [Accessed: 20th January 2018]

About the authors

Mr. SARON MESSEMBE OBIA is an Author and Expert in International Security and Terrorism, and IREX Artificial Intelligence Expert (IREX AI- U.S). Executive Director of Intelligence Security Solutions and Theorist Coordinator at Cyber Jurisprudence International Initiative Sohag-Egypt. 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'; 'Online Services and Lab Glass: Forensic Investigation and Cloud Computing' and Weaponized Drones Terrorism in Africa Al Qeada, Al Shabaab, Boko Haram & ISIS'

Dr. AIGBE DIYELI SEGUN is an experienced criminologist and security professional with a demonstrated history of working in the research and security sector industry in Nigeria and Africa. A dynamic and versatile security professional with over 15 years of experience in the security sector. He built a track record of managing a very successful network. The National Network for Safe Communities and Civil Society Organizations (CSO) to support citizen's implementation process for strategic intervention to violence and improve the relationship between law enforcement among INNER CITY GANGS, especially in the implementation of violent Acts among Gangs through Project Heal: A Drug Market Intervention Programme. He Holds an MSc from University of Ibadan in Criminology and Security Psychology. His PhD is in Criminology from the University of Calabar, Cross River State, Nigeria, with a special interest in criminal profiling, criminal psychopaths and counter-terrorism in the Horn of Africa, Lake Chad Basin and Sahel Region respectively.

RIEAS PUBLICATIONS

RIEAS welcomes short commentaries from young researchers/analysts for our web site (about 700 words), but we are also willing to consider publishing short papers (about 5000 words) in the English language as part of our publication policy. The topics that we are interested in are: transatlantic relations, intelligence studies, Mediterranean and Balkan issues, Middle East Affairs, European and NATO security, Greek foreign and defense policy as well as Russian Politics and Turkish domestic politics. Please visit: www.rieas.gr