Hacking as a socio-political menace in Cameroon

Saron Obia [1 A]

[A] Pan African Institute for Development, West Africa (PAID-WA), Buea, Cameroon

Received: December 16, 2021 | Revised: December 27, 2021 | Accepted: December 30, 2021

DOI: 10.33445/sds.2021.11.6.13

Abstract

The globalization era is contributing factor for sustainable development in Sub Saharan Africa. With the incorporation of e-banking, e-commerce, and e-learning, several security challenges are yet to be solved, such as; hacking of bank accounts and institutional websites. The enemy is not far. This paper explores how criminals seek justice from state machinery through social engineering and security breach. It also discusses on the vulnerabilities of public service infrastructures in Cameroon. However, the paper appeals on the fact that, despite existing laws and the creation of security organizations to monitor and control system in the country, the emergence of cybercrime is yet another challenge, as that of terrorism.

Key words: hacker, cybercrime, election Cameroon, Boko Haram.

Introduction

Civilizations began in Africa, and the continent is hybrid for scientist. Cameroon is amongst Sub Saharan African countries which embraced the technological innovation era. The digital pandemic of cybercrime has not only affected Europe, but has extended to Africa, with hackers gaming the system in Cameroon. Located in Central Africa, with surface area of 475 442 km² and total population of 24,229,247 as of 31 December 2017, with 12114634 (50.1%) females and 12,114613 (49.9%) males (Ngang Eric, 2018). Cameroon has a growing population, made up of youths and its density is 52.2 people per square kilometer (135.3/mi2) (NAICT 2007), with Yaoundé and Douala housing a huge population due to socio-political crisis in the country.

According to the National Agency for Information and Communication Technologies (ANTIC), Information and Communication Technology (ICTs) has reconfigured developing countries, thereby creating new opportunities for youths. These opportunities which support sustainable development through local and international connectivity of individuals, communities, and private sector, with the assessment, utilization and sharing of information and knowledge via different networks.

In the bid to consolidate technological evolution dynamics, Cameroon introduce several initiatives for the development and deployment of ICTs. Which are but not limited to:

- The implementation of an ICT development programme by the Ministry of Higher Education. With authority of the president, the distribution of electronic devices (laptop) to university students and other private higher education institutions;
- The creation of multimedia training centres in secondary schools and digitalization of fees online implemented by the Ministry of Secondary Education;
- The computerization of passport and national identity card by the Delegation of National Security;
- The computerization of the electoral process by the Ministry of Territorial Administration and Decentralization.

[1] **Corresponding author**: MSc in Security Studies and PGD in Criminology and Security Management, e-mail: princemessembe@gmail.com, ORCID: 0000-0002-3878-9313

The global economy is interconnected with national and international initiatives to support the groove of the digital era, such as:

• the initiative of the Economic Commission for Africa (ECA) with focus on National Information and Communication Plan (NICI Plan);

• the UNDP initiative on an ICT policy in Cameroon within the framework of the Second Tokyo International Conference for African Development (TICAD II).

These projects have changed the telecommunication and business infrastructures in the sub-region, and Cameroon in particular, encountering to a digital pandemic. The development of electronic transactions such as mobile payment or electronic wallet, biometric identity cards, and biometric passport. This development which is accompanied by new training niches in universities with the creation of new specialized majors to provide Cameroonians with highly qualified human resources in the field of ICT and as well combat emerging crimes (Atsa et al. 2016).

From period 2008-2017, marked the reconfiguration of Cameroon telecommunication infrastructure, for a better coverage, network for users and better services for clients. There has been migration from the 2G saga (Voice and Short Message System "SMS"), then the migration to 3G (September 2014) which boosted networks quality and innovative services integrating multimedia applications. The entry in to the fourth generation (4G) service in 2015, has reorganize the mobile telephony landscape, leading to the emergence of a new digital economy (Bahri-Domon 2017). CAMTEL engage diverse partners to enhance Internet access at an affordable rate. For example, CAMTEL's blue service (2021 service created by CAMTEL) and the signing of commercial agreement with data service provider Yoomee on 22 February 2017, with national telecom operator CAMTEL, making Yoomee becoming an official Mobile Virtual Network Operator (MVNO) in Cameroon, with major issue; affordable data services to the entire Cameroonian market and effective deployment of optical fibers network.

Cameroon major network operator CAMTEL using its connection to the SAT3 is gradually deploying the optical fibre technology to enable Internet connectivity, critical in the development of telecommunication services. The West Africa Cable System(WACS) project, deployed by MTN Cameroon and implemented by a local subsidiary of the Orange group, with objective to enable the latter boost of an urban and inter-urban optic fibre network estimated at roughly 6,000 kilometres, forecasted by the government to be increased to 10,000 kilometres by 2020, thus making the nation a hub for telecommunication infrastructure in Central Africa (Business in Cameroon 2017, Atsa et al. 2016, CC_PRC, 2016).

Results and discussion

Landscape of telecommunication in Cameroon

The period 1960-1988

In the 1960s, Cameroon telecommunication sector was controlled by MINPOSTEL, in charge of orientations, regulation, control, monitoring operations of telegraphy, and telephony. The fast incorporation of telecommunication led to the creation of the National Advanced School of Post and Telecommunication (ENSPT) in 1969 and the International Telecommunications of Cameroon (INTELCAM) in 1972. The Head of State passed into law No. 87/021 of December 17 1987 granting financial autonomy to MINPOSTEL to enhance efficient of management and improve telecoms services, to match international standard.

The period 1989-1998

From this period, Cameroon gradually engaged in the digitalization of some sector, such as; the Yaoundé and Douala Digital Exchange Stations followed by the South West Station. The inertia within the telecommunications sector Nationwide,

prompted the adoption of legislation in order to reconfigure the sector and related institutions in 1998. Below is some legislation which empowered the telecommunication sector:

• Law No. 098/14 of July 14, 1998 relating to creation of a new legal and regulatory Telecommunication framework, leading to competition on internal markets in the sector;

• Decree No. 98/198 of 8 September 1998 to set up the Cameroon Telecommunications Corporation (CAMTEL);

It is worth noting that in 1998, CAMTEL emerge from a fusion between Department of Telecommunications of MINPOSTEL with INTELCAM, rendering exclusive rights on the operation and provision of fixed telephone services. However, this legal screen and institutional reform are yet to yield substance, due incoherent implementation strategies to develop the sector, insufficient resources, poor involvement of national and international actors (The Sector Strategy for Telecommunications and ICT 2005 – 2015, NAICT 2007).

The period 1998 to date

From 1990s till date, Cameroon's Head of State adopted a radical shift in the promotion of telecommunication and ICT. In order to meet up with other develop countries and restructure state economy, several laws were enacted not only for proper digital economy but also to face new challenges, these laws are but not limited to:

• Law on the prescription of minimum services in the communication sector in 2001 (NA_MSC, 2001);

• Decree No. 2001/830/PM of 19 September 2001 to lay down modalities for the operation of telecommunications networks;

• Decree No. 2001/831/PM of 19 September 2001 to lay down modalities for the provision of telecommunications services;

• Law No. 2001/10 of 23 July 2001 to institute minimum service in the telecommunications sector;

• Law No. 2005/13 of 29 December 2005 to amend and supplement some provisions of Law No. 98/14 of 14 July 1998 to govern telecommunications in Cameroon.

In a dynamic statement in 2004, the Head of State declared that "Our country needs generalized access to the Internet", not only to boost digital economy of the state, but to lead Cameroonian youths in to e-business and develop new skills (Silicon Mountain in Buea and Active Space, a hub for tech giants in Cameroon), for the protection consumers and provide solutions to emerging security challenges. The set of law include:

• 2010 Law relating to electronic communication (NA_EC, 2010). This law seeks to promote universal service in the country. Under the law, Cameroon's telecommunications operators are required to provide "communications services of good quality, at affordable rates, and in an uninterrupted manner.";

• Law No 2010/012 of 21 December 2010 relating to cyber security and cyber criminality in Cameroon

• 2011 Law on consumer protection (NA_CP, 2011). This Law was enacted to protect consumers by providing for individual or collective legal action, authorizing the Cameroon's telecommunications regulator, the Telecommunications Regulatory Board (TRB) to be responsible for mediation and settlement of conflicts in the case of noncompliance by operators (AI4A 2014).

Cyber security and cyber criminality landscape in Cameroon

Law No 2010/012 of 21 December 2010 relating to cyber security and cyber criminality in Cameroon, in its section 4 provides contextual definitions and implementation of the law in relation to criminal patterns, such as; illegal access, active attack, passive attack, integrity violation, security audit, authentication, illegal content and denial of service.

Part 2, Chapter 1 of the law focuses on electronic security and general security issues. But section 6 reaffirms the provision in section 4(2), which gives the Ministry of Post and Telecommunications the power to formulate and enforce electronic communication policy.

Chapter 2 of the 2010/012 law focuses on regulation and monitoring of electronic security activities. section 7, provide that, ANTIC shall be the police for electronic security activities

(section 7 (2)).

The digital pandemic in Cameroon, particularly in the domain of information security can be traced to the year 2000, with the advent of cybercrime and identity theft. With troubling statistics revealed by ANTIC, on the vulnerability rate of Cameroon, based on the fact that, most of the software used in the country has been hacked. There is no doubt that new security measures need to be developed in order to combat the menace of identity theft, and hacking in particular as per section 24, per Law No 2010/012 of 21 December 2010 relating to cyber security and cyber criminality in Cameroon.

The menace poses by cybercriminal in Cameroon

Information and communications technology (ICT) are an emerging challenge for developing countries. According to Nyangosi, Arora & Sumanjeet (2009:82), e-banking has become global. This system, provides fast delivery of banking services to a wide range of customers. The Internet, one of the most successful innovations in the world, has created numerous opportunities, as well as threats for organizations (Chau & Lai, 2003).

Atsa et al., (2016) concluded that, the reconfiguration of enterprises and institutions to emerge economically in Cameroon, appeals for the implementation of multi sectoral and multi actor approach from the analysis of the 7 pillars of a digital economy. The need to incorporate digital technology in businesses, and establishments is necessary for companies which operate with new services such as; social media, cloud computing and massive data, open data (public and private), exploitation of optical fiber and 4G networks, organize competitions for civic groups to challenge the regulatory and operational environments, in other to adapt to new trends. Although the Ministry of Posts, Telecommunication and other state institutions have launched several projects to enhance access, and security of key infrastructures in Cameroon, more is still expected, cybercriminals continue gaming the system (hacking, identity theft, and SIMBOX scam). Some cases of hacking in Cameroon are explored below.

Hacking of CAMAIR-CO 2011

The advent of technology has changed security dynamics in the world, as most countries are been hit by cyber-attacks, causing huge financial loses. In 2011, Cameroon leading flight CAMAIR-CO, system was breached by unscrupulous individuals, who succeeded to establish several flight tickets with the travelling agency trademark. This incident prompted the state to focus on issues relating to cyber security with the MINPOSTEL and ENIX (cyber security structure) to ensure the security of international and national entities from cyber breach.

Despite resource put in place, cybercriminals continue to double efforts, as more state systems are been breach, not isolating airtime theft (SIMBOX), financial lost both by mobile operating companies and users, phishing and SMISHING.

More so, director of legal affairs of Microsoft for West and Central Africa, Serge Ntamack, out pinned that, the emergence of cyber criminality in Cameroon, is because 83% of software used in the country have been compromised. A research conducted by International data corporation (IDC) and University of Singapore (NUS), revealed that cybercriminal activities amount to 175 000 milliards XAF per year. This major security challenge has led to the adoption of laws to provide evidence and prosecute individuals engage in such acts.

Hacking of Cameroon national assembly 2012

In 2014, Cameroon parliament website was hacked, with pro-gay message which reads: 'Stop persecuting homosexuals' (https://www.camerounweb.com/CameroonHomePage/NewsArchive/CMR-parliament-website-allegedly-hacked-by-vengeful-gay-311953). The penal code sanction acts between a male and male, as well as a female and another female. It appeals that, the hack was orchestrated by pro-gay (collective Wholeop Crew), to advocate against the prosecution of their 'partners'. This act lead to the deactivation of the site, though the assembly denied 'conspiracy theory' and assembly computer scientist confirmed the hack.

The message of the hack website (at the

time) read: 'Hacked, quite simply. 'WebSite defaced 'I've no limit 'I have gained full access to your server. 'I got all your data. 'Stop the persecution of homosexual people 'Template WholeOp Crew 'THE END' (https://www.camerounweb.com/CameroonHomePage/NewsArchive/CMR-parliament-website-allegedly-hacked-by-vengeful-gay-311953).

An assembly staff told Agence Ecofin, 'The damage has been done.' 'It was still public web address of the National Assembly, an institution of the Republic'. Though not the first in the country, because the site was designed with poor version of Joomla. However, some civil society organizations and lawyers continue to prone for the rights of gays and they are yet to obtain such prescription from the legislator, and cybercrime is punishable in Cameroon.

Hack Presidential Website 2015

The vulnerability rate of software used in Cameroon, pose a major security menace, that of social engineering or cyber breach of profiled institutional websites (notably that of the presidency). On March 2015, a fabricated photo was uploaded on the website of the presidency, a photo of the Head of State, (while on vacation in Europe) honoring some gallant soldiers killed by Boko Haram jihadists. Whereas, on 6 March 2015, he was represented by the Minister Delegate at the Presidency in charge of Defense, Edgar Alain Mebe Ngo'o. The minister equally decorated the soldiers posthumously with different titles, but on the website of the presidency days after, the fabricated photo appeared. The photo created so much controversy with local newspapers, bloggers, and politicians rebuking administration.

Source: Saron Obia (2021) adapted from Eden Newspaper

In a press release on 11 March, the Minister of Communication and government's spokesperson, Issa Tchiroma, claimed the presidential website was compromised or breach. He further emphasized; "We are conscious of the gravity of such a picture whereas the head of state is in Europe. The photo was intentionally modified by a malicious hacker. It is impossible that it is done by someone from inside because everybody knows that president Biya is not around". This incident appeal for update of Cameroon's cyber security policing method.

Hacking of Elections Cameroon (ELECAM) 2020

The hacking of ELECAM was quacking linked to opposition party, view the message and photo posted by the hacker (correlation to the message of an electoral hold up in Cameroon). The post on the website read "In reaction to the presence in recent hours of an image of President-elect Maurice Kamto on the official Facebook account of Elections Cameroon (Elecam), the President-elect warns activists and supporters of the CRM against this malicious manoeuver of manipulation and division.

Therefore, he urges them not to fall into this trap." The President of the electoral board of Elections Cameroon, Enow Abrams Egbe reacted officially to the situation, in a Communique signed Wednesday June 24, 2020, and place a red notice to track down the criminals engaged in the act.

On august 2020, two men, Tata Derrick and Vedzedze 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 detained at the judicial police headquarters in Yaoundé for over four days, the two confessed to have hacked the Facebook page of Elections Cameroon (ELECAM) on June 23, 2020. Hacking is an emerging menace which needs to be stopped by engaging security experts, researchers, IT specialists and ethical hackers to redefine Cameroon's institutional security to face new global challenges.

Hacking of administrative authorities in the West region of Cameroon 2021

On May 27, Governor Awa Fonka Augustine, through a radio announcement revealed that his Orange phone number was hacked by cybercriminals. They exploited the opportunity to extort money from people and organizations. The hack occurred on May 26th 2021 around 10AM. He appealed to the public to be aware if anyone receives a call or any other request from the number to be ignored and be signaled to law enforcement. Investigations were opened by the Legion Gendarmerie in collaboration with other security departments, in the East region, police and the Direction General de La Recherché Exterieure (DGRE).

Known for its best policing approach, the joint efforts led to the arrest of suspects just after three weeks of investigation. Three of the suspects were apprehended in the East region, one in Garoua-Boulai and two in Bertoua and the last suspects in Yaoundé (Journal du Cameroun, 2021). Five of them were retained, including a woman and presented to the press on Tuesday June 15 AT the Special Unit for Criminal Research and Investigation of Bafoussam, while awaiting judgement.

Similarly, the mayor of Mbouda, in the West region, WhatsApp account was hacker by cybercriminals on Saturday 19th June 2021, leading to extortion of friends and family members of Mayor Wandji (During an interview with the CEO of Cameroon News Agency of June 2021, social engineering is one of the methods used by cybercriminals for victimization). It was also revealed by the Cameroon News Agency that, cybercriminals succeeded to extort FCFA4million. The mayor filed a complaint on Monday 21 June 2021 at the judicial police of Bafoussam awaiting the crackdown of the fraudsters.

Conclusions

There is growing evidence that banks and customers benefit substantially from e-business and new technologies, the Internet in particular (Zorayda, 2003:33). Banks like any other national and international organization, need to ensure the privacy of clients and workers are not at stake. Law No 2010/012 of 21 December 2010 relating to cyber security and cyber criminality in Cameroon, Section 41 and Section 42 focuses on the protection of privacy. Section 66 (1), (2), and (3) sanctions criminal maneuver.

Section 66. (1) Whoever causes disturbance or disruption of the functioning of an electronic communication network or a terminal device by introducing, transmitting, destroying, erasing, deteriorating, altering, deleting data or rendering data inaccessible shall be punished with imprisonment for from 02 (two) to 05 (five) years or a fine of from 1.000.000 (one million) to 2.000.000 (two million) CFA francs or both of such fine an imprisonment.

(2) Whoever uses the deceptive or undesirable software to carry out operations on a user's terminal device without first informing the latter of the true character of the operation which the said software is likely to damage shall be punishable with the same penalties.

(3) Whoever uses potentially undesirable software to collect, try to collect or facilitate any of such operations in order to access information

of the operator or supplier of an electronic network or services and commit a crime shall be punishable in accordance with subsection 1 above.

Moreover, most cybercriminal succeed because of staff dishonesty in financial institutions (where some act as pick-up). Section 73 (1) of the 2010/012 law lay down sanctions on such behaviors, which are related to uses an information system or a counterfeit communication network to falsify payment, credit or cash withdrawal card or uses or attempts to use, in full knowledge of the facts, a counterfeit or falsified payment, credit or withdrawal card shall be punished with imprisonment for from 02 (two) to 10 (ten) years and a fine of from 25,000,000 (twenty-five million) to 50 000 000 (fifty million) CFA francs or both of such fine and imprisonment.

Though hacking is not new, it's an emerging menace for youths and the administration in Cameroon. From the series of hacking above, the state through decentralized channels like ANTIC, must develop new security strategy to ensure security data is not compromised. The creation of digital forensic center in Buea, is just the first step, but the creation of a taskforce of hackers and security experts (criminal investigators) to develop and implement adequate measures will help apprehend criminals.

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

Chau, K.Y., Lai, P., & Vincent, S.K. (2003). An empirical investigation of the determinants of user acceptance of Internet Banking. Journal of Organizational Computing and Electronic Commerce, 13 (2): 123-145.

CRTV 2018, Major announcements in the head of states message to the nation. Available from: http://www.crtv.cm/2018/01/major-announcements-in-the-head-of-states-message-tothe-nation/

Dutta S., Baller, S., and Lanvin, B. (2016) The Global Information Technology Report 2015:

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,

Ngang Eric, N. 2018. Assessing the Socio-Economic Impact of Internet Shutdown in The English-Speaking Regions of Cameroon from A Multistakeholder and Multisector Perspective

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

P.R.C (2016) Digital economy: A great gift of the Head of State to students, Republic of Cameroon, Presidency of the Republic. Available from: https://www.prc.cm/en/news/1870-digitaleconomy-a-great-gift-of-the-head-of-state-to-students

National Agency for Information Communication Technology (NAICT) (2007), National Policy for the Development of Information Communication Technology, [Online] Available from: http://www.istafrica.org/home/files/Cameroon_NationalICTPolicy_2008.pdf

Law nº2010/013 English version. Available from: http://www.art.cm:81/images/doc/lce%20version%20anglaise.pdf

Law nº2011/012 Framework on Consumer Protection. Available from: http://www.digitcamlaws.net/GICAM/Law_framework_on_consumer_protection_in_Cameroon.pdf

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