Africa Online & Publication Library

FIGHTING CYBERCRIME IN CAMEROON: A LEGAL AND CYBERSECURITY PERSPECTIVE

Author: Ngenge Ransom Tanyu

Policy Brief

Series 2, No 1, September 2023

Opinions expressed in this paper are those of the author(s) and do not necessarily reflect views of the organisation.

IMPRESSUM

Africa Online & Publications Library
Gikondo, Kicukiro, Umujyi wa Kigali, RWANDA

Tel: +237681757380
Emails: info@africaopl.org, contact@africaopl.org
Website: https://www.africaopl.org/

Papers can be downloaded free of charge from the AOPL website:
https://www.africaopl.org/publications/categories/policy-briefs

Fighting cybercrime in Cameroon: A legal and cybersecurity perspective

Author: Ngenge Ransom Tanyu

PhD candidate at the Pedagogical University of Krakow

Key Highlights

- Cybercrime is on the rise in Cameroon, with far-reaching consequences for individuals, businesses and national security.
- Cameroon lost XAF12.2 billion in 2021 to cybercrime, including losses from intrusion, scams, phishing and banking card skimming.
- Business email compromise (BEC) attacks are a major threat to companies in Cameroon.
- Cameroon has taken steps to address cybercrime through comprehensive legislation and its accession to the Budapest Convention on Cybercrime.
- Internet users are recommended to follow specific security measures, such as keeping software updated, using strong, unique passwords and being cautious with email attachments and suspicious links.
- Collective efforts from government institutions, private businesses, and citizens are essential to enforcing laws, reporting cybercrimes and investing in cybersecurity measures.
- Increased awareness and action at individual, corporate and state levels are crucial to safeguarding Cameroon's digital landscape.

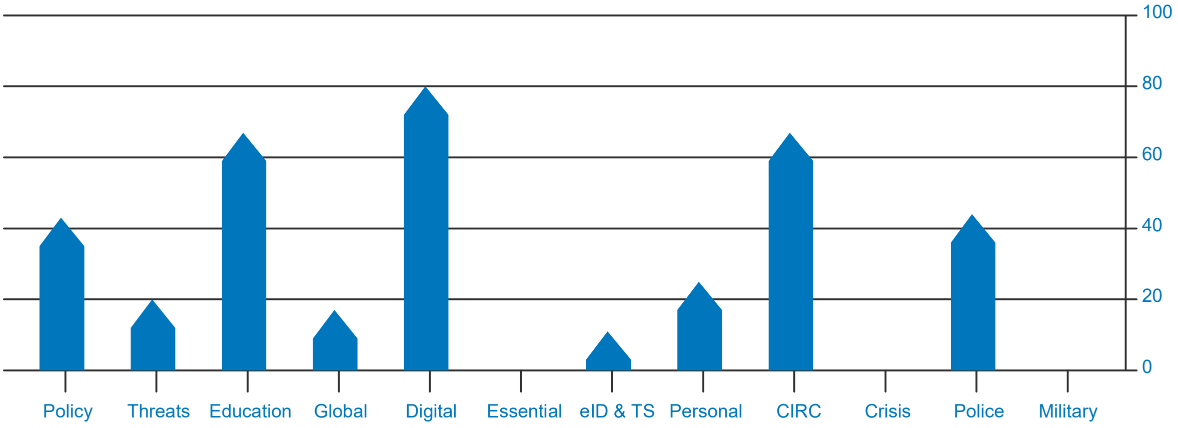
1 Introduction

Two years ago, the market value of cybersecurity in the Middle East and Africa stood at a whopping $1.98 billion, according to statistics from Expert Market Research (EMR 2022). This market is projected to expand at a compound annual growth rate (CAGR) of 7.90% from the 2023 to 2028, reaching a value of $3.12 billion by 2027 (Fernando 2022). Although limited bandwidth and poor internet access continue to hold back Africa's transition to a digital economy, it is heartbreaking to know that this has not halted cybercrime on the continent, which is now one of the largest problems faced by governments, private businesses and individuals. In today's increasingly digitalised world, peace and security can be used to symbolise not only the absence of cyberwar and cyberespionage but also the negative effects of cybercrime, which include scamming, phishing, identity theft, amongst others. Ngando (2022) and Andzongo (2022)**,** for instance, state that fake news, personal or administrative data leakages, and bank card frauds have become daily occurrences in Cameroon, given the country's massive number of internet users, with 21.69 million people owning a mobile phone, 10.05 million of whom are internet users, and 4.55 million of whom are active on social media, according to the National Agency for Information and Communication Technologies (ANTIC). In this briefing, I touch on the many cybercrimes prevalent in Cameroon and explain how they undermine peace and security, as well as provide cybersecurity techniques that private companies, government institutions and individuals can use to protect themselves, their businesses and sensitive data.

2 State of digitalisation in Cameroon

The National Cyber Security Index (NSCI) based in Tallinn, Estonia, ranks Cameroon 96th on the NSCI index, 93rd on the Global Cybersecurity Index, 149th on the ICT Development Index, and 114th on the Networked Readiness Index, giving 32, 46, 24 and 33 percentages, respectively (Velasco 2022). The data are based on a timeframe of 2021–2023, with the NCSI fulfilment rate shown in the graphic below.

NCSI fulfilment percentage[1]



Cybersecurity indicators throughout Cameroon suggest that cybersecurity policy development is at 43%, cyber threat analysis and information is at 20%, education and professional development is at 62%, and contribution to global cybersecurity is at 17%.

For baseline cybersecurity metrics, protection of digital services is at 80%, protection of critical services is at 0%, e-identification and trust services are at 11%, and personal data protection is at 25%.

Cyber incident response is 67%, cyber crisis management is 0%, fighting cybercrime is 44%, and military cyber operations are 0%, according to incident and crisis management indicators.

A close assessment of the statistics above reveals that, despite significant progress in the educational and professional development of cybersecurity, the protection of digital services and the response to cyber incidents in Cameroon, all other critical aspects of its digital economy, such as military cyber operations, the protection of essential services, and the fight against cybercrime, fall below 50%.

3 Cybercrime in Cameroon

As far back as 2010, Cameroon was already ranked number one worldwide for online fraud by McAfee (Matseke 2010). McAfee found that more than one-third of the websites hosted in Cameroon are suspect, making it the world's most dangerous place for Internet users to browse, surpassing China, Samoa, the Philippines and Russia (IT News Africa 2010). Despite recent reports of new rules the government has passed to fight cybercrime, little has changed. AllAfrica (2022) states that 61% of

[1] Velasco, P. (2022).

cybercrimes in Cameroon are scams, compared to 27.80% for phishing, 2. 30% for intrusion, 4. 10% for cyber blackmail and 3. 60% for cyberbullying.

In Cameroon, online abuse of women is another serious and prevalent problem. According to Internews' 2021 situational analysis of digital security in Cameroon, a whopping 77% of women reported being the target of online abuse (Fischer 2021). These occurrences take the form of stalking (75%), sexual harassment (69%), and intentional embarrassment (19%), including revenge porn and derogatory name-calling. The respondents, who make up 73% of the sample, feel that they were singled out due to their gender.

In other words, nearly three-quarters of women in Cameroon have been harassed or abused online. This abuse can take many forms, including stalking, sexual harassment and public humiliation. The perpetrators often target women because of their gender.

3.1 Negative impact of cybercrime

Business data recently released by ANTIC suggests that Cameroon lost XAF12.2 billion to cybercrime in 2021, which is roughly twice what was seen in 2019 (Andzongo 2022, 1). To quote her:

> *A detailed review of the 2021 figures shows financial losses amounting to XAF2.5 billion caused by intrusion into the public and private IT systems. Scam and phishing caused XAF6 billion losses while skimming (copying banking cards' data by installing specific equipment on ATMs) caused a XAF3.7 billion loss. In 2020, ANTIC published a report showing close to XAF6 billion was lost to bank fraud in 2019.*

BEC, a type of email scam, was the most common way in 2021 for criminals to impersonate executives and steal money. The agency said that early signs of a BEC attack include an urgent request for a financial transfer, a change in contact information or direct contact from a scammer pretending to be a company employee or manager. In 2021, an ANTIC assessment found 27,052 vulnerabilities in the IT systems of public and private agencies.

4 Fighting cybercrime in Cameroon

Cybercriminality and cybersecurity in Cameroon are regulated by Law N° 2010/012 of December 21, 2010 (Official Gazette of the Republic of Cameroon 2010). In the

General Provisions of the Law (Part 1, Section 4, paragraphs 32 and 33), cybercriminality and cybersecurity are defined as follows (Official Gazette of the Republic of Cameroon 2010, 7):

> *Cybercriminality: an infraction of the law carried out through cyberspace using means other than those habitually used to commit conventional crimes;*
>
> *Cybersecurity: technical, organisational, 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;*

Chapter I, Part III of Cameroon's cybercrime law, details the procedural law provisions relating to cybercriminality. The various steps to be taken in case of any cyberoffence include, but are not limited to:

- Opening of a criminal investigation
- Police can search for and seize data related to cybercrime, either physically or electronically.
- This data can be used as evidence in court, but it must be collected and stored in a way that preserves its validity.
- Setting up a rotatory commission at the national and international level, any corporate body or natural person to search the elements of cybercrime offences of which at least one of the elements was committed on Cameroonian territory or which one of the offenders or accomplices resides on the said territory.

Chapter II, Part III of the Law focuses on the crimes and punishments related to cybercrime. The severity of the punishment depends on the magnitude of the crime, the data breach(s) involved, and the personalities or companies affected. Punishments can range from three months to ten years imprisonment, fines from 20,000 to 100,000,000 CFA francs or both.

Other laws that offer protective measures against cybercrime include:

- Law No. 2022/002 of April 27, 2022, which authorises the President of the Republic to proceed with Cameroon's accession to the Budapest Convention on Cybercrime

- Decree No. 2022/169 of May 23, 2022, proclaiming Cameroon's accession to the Budapest Convention
- Constitution of the Republic of Cameroon, amended by Law No. 96-06 of January 18, 1996, which guarantees privacy of communications in its preamble
- Criminal Procedure Code of 2005, established by Law No. 2005/007 of July 27, 2005
- Section 1 of the Law N°2010/012 on Cybersecurity and Cybercrime states that it seeks to “protect basic human rights, in particular the right to human dignity, honour, and respect for privacy, as well as the legitimate interests of corporate bodies”.
- Law N° 2005/007 of July 27, 2005, provides cross-cutting safeguards.

Disputably, Cameroon has a comprehensive cybercrime law in place, which is supplemented by other laws that offer protective measures against cybercrime.

Even though it is difficult to know how well Cameroon’s cybersecurity law is being enforced, the fact that it exists shows that Cameroon takes cybersecurity seriously. In addition to the law, ANTIC (2023) recommends the following 10 commandments for Cameroonian internet users to take basic precautions to protect their computers and other devices from attacks.

I. **Use of strong passwords.** A strong password is at least 8 characters long and includes a mix of upper and lowercase letters, numbers, and symbols.

II. **Regular software updates.** Software updates often include security patches that can help protect computers from known vulnerabilities.

III. **Do regular data backups.** In the event of a cyberattack, a data backup can help in recovering lost data.

IV. **Deactivate ActiveX and JavaScript components.** ActiveX and JavaScript components can be used by attackers to exploit vulnerabilities in computers. It is best to disable them by default and only enable them when needed.

V. **Do not be in a haste to click on links.** Phishing emails and malicious websites often contain links that can download malware onto computers. Be careful about clicking on links, especially if they come from unknown senders.

VI. **Never use an administrative account to navigate.** An administrative account has full control over computers, so it is important to only use it when necessary. For everyday tasks, use a standard user account.

VII. **Control access to online accounts.** Always sign out of online accounts after using them, especially when using a public computer. Use strong and different passwords for all online accounts.

VIII. **Never share a hoax.** Hoax emails and messages often contain malicious attachments or links. Be careful about sharing any information online, especially if it comes from an unknown source.

IX. **Be careful.** The internet is a dangerous place, so it is important to be vigilant when you are online. Be careful about what information you share and what links you click on.

X. **Be careful while opening attachments to an email; they often have malicious codes.** Email attachments are a common way for attackers to spread malware. Be careful about opening any attachments, especially if they come from an unknown sender.

To expand on the ANTIC guidelines, internet users in Cameroon should also take special note of the following cybersecurity measures to protect themselves and their data online:

- Use two-factor authentication (2FA) whenever possible. 2FA adds an extra layer of security by requiring a code from your phone or another device in addition to your password when logging in to an account.
- Use virus and malware protection software. Keep your antivirus and anti-malware software up to date to protect your devices from viruses, Trojans and other malicious software.
- Use a VPN on public Wi-Fi. A VPN encrypts internet traffic, making it more difficult for snoopers to steal your information.
- Only use reliable websites and services. Look for the HTTPS or SSL icon in the address bar to make sure that a website is secure.
- Adjust social media privacy settings. Limit the amount of personal information that is publicly visible on your social media profiles.

- Stay informed about the latest cybersecurity threats. There are many resources available online and in libraries that can help you learn about the latest cybersecurity threats and how to protect yourself.
- Attend cybersecurity training sessions and consult with specialists if necessary.

5 Conclusion

More than cybersecurity education and professional development, adopting laws and decrees, and establishing a national cybersecurity commission are required to fight cybercrime in Cameroon. It will take the joint efforts of government institutions, private businesses and citizens to ensure that current cybersecurity laws are implemented and respected, cybercrimes are reported when discovered, and private companies invest in and set up cybersecurity management systems. The objective of this paper was to create further awareness of the importance of cybersecurity action in Cameroon at individual, company and state levels.

Funding

The research for this paper was funded by the PROM programme of the Pedagogical University of Kraków, Poland. The PROM programme is a mobility programme that supports the participation of PhD students and researchers in international scientific conferences and summer and winter schools.

References

AllAfrica. 2022. "Cameroon: With Cyber Fraud on the Rise, Customer Security Remains Essential." *AllAfrica*, September 22, 2023. https://allafrica.com/stories/202210250108.html.

Andzongo, Sylvain. 2022. "Cameroon Lost XAF12.2 Bln to Cybercrime in 2021 (ANTIC)." *Business in Cameroon*, February 4, 2023. https://www.businessincameroon.com/public-management/0703-12393-cameroon-lost-xaf12-2-bln-to-cybercrime-in-2021-antic.

ANTIC. 2023. "10 COMMANDMENTS OF INTERNET SECURITY." *National Agency for Information and Communication Technologies*, September 22, 2023. https://www.antic.cm/index.php/en/security/best-practice.html#.

EMR. 2022. "Middle East and Africa Cybersecurity Market Report and Forecast 2023-2028." *Expert Market Research*, January 30, 2022. https://www.expertmarketresearch.com/reports/middle-east-and-africa-cybersecurity-market.

Fernando, Jason. 2022. "Compound Annual Growth Rate (CAGR) Formula and Calculation." *Investopedia*, May 24, 2023. https://www.investopedia.com/terms/c/cagr.asp.

Fischer, Mark. 2021. "Situational Analysis of Digital Security in Cameroon." *Internews*, February 4, 2023. https://internews.org/resource/situational-analysis-of-digital-security-in-cameroon/.

IT News Africa. 2010. "McAfee: Cameroon Has the Web's Riskiest Domain." *IT News Africa*, September 22, 2023. https://www.itnewsafrica.com/2010/02/mcafee-africa%E2%80%99s-cameroon-the-web%E2%80%99s-riskiest-domain/.

Matseke, Palesa. 2010. "Cameroon Tops Internet Security Fraud List." *defenceWeb*, January 26, 2023. https://www.defenceweb.co.za/industry/industry-industry/cameroon-tops-internet-security-fraud-list/.

Ngando, Esther Sillo. 2022. "Cybersecurity / Cybercriminality, P&T Family Recommend Emergency Plan." *MINPOSTEL,* January 27, 2023. https://www.minpostel.gov.cm/index.php/fr/actualites/408-cybersecurity-cybercriminality-p-t-family-recommend-emergency-plan.

Official Gazette of the Republic of Cameroon. 2010. “Law No 2010-12 of 21 December Relating to Cybersecurity and Cybercriminality in Cameroon”. *Ministry of Justice*, September 22, 2023. http://www.minjustice.gov.cm/index.php/en/instruments-and-laws/laws/302-law-no-2010-12-of-21-december-relating-to-cybersecurity-and-cybercriminality-in-cameroon.

Velasco, Paola. 2022. “104. Cameroon 32.47.” *National Cyber Secuirty Index*, January 28, 2023. https://ncsi.ega.ee/country/cm/.