NOTES
DE L'IFRI

AOÛT
2026

La cybercriminalité en Afrique centrale

Typologie, expériences et gestion par les pouvoirs publics

Centre Afrique subsaharienne

Philippe AWONO EYEBE

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une fondation reconnue d'utilité publique par décret du 16 novembre 2022. Elle n'est soumise à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

Note réalisée par l'Institut français des relations internationales pour la Direction générale des relations internationales et de la stratégie du ministère des Armées.

Elle a été réalisée dans le cadre du partenariat entre l'Observatoire de l'Afrique centrale et orientale et l'Institut français de recherche en Afrique (IFRA-Nairobi).

ISBN : 979-10-373-1261-7

Comment citer cette publication :
Philippe Awono, « La cybercriminalité en Afrique centrale : typologie, expériences et gestion par les pouvoirs publics », *Notes de l'Ifri*, Ifri, août 2026.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Auteur

Philippe Awono Eyebe est enseignant-chercheur de science politique à l'université de Yaoundé II qu'il a rejoint après l'université Jean Moulin Lyon 3. Il est responsable adjoint du séminaire Intégration régionale à l'École supérieure internationale de guerre de Yaoundé, directeur exécutif de l'Observatoire du politique en Afrique et directeur du Centre de recherches pluridisciplinaires sur l'Intelligence artificielle (CREPIA), membre de plusieurs réseaux de recherche dont le Réseau d'étude sur la globalisation et la gouvernance internationale et les mutations de l'État et des nations (REGIMEN).

Il a publié une dizaine de textes scientifiques dans des ouvrages et revues à comité de lecture. Ses centres d'intérêt concernent la Francophonie, la gouvernance des organisations internationales, la sécurité internationale et la gouvernance de l'Intelligence artificielle.

Résumé

La présente *Note* examine la montée en puissance de la cybercriminalité en Afrique centrale et la réponse des États concernés. Les principales conclusions sont les suivantes :

- la cybercriminalité augmente et devient de plus en plus sophistiquée ;
- la petite et la grande cybercriminalités sont caractérisées par des acteurs, des cibles et des méthodes différents ;
- les pouvoirs publics bâtissent progressivement une politique de cybersécurité ;
- cette politique néglige encore certains aspects clés de la lutte contre la cybercriminalité.

Abstract

This study examines the rise of cybercrime in Central Africa and the response of the countries concerned. The main conclusions are as follows :

- cybercrime is on the increase and becoming more sophisticated;
- small- and large-scale cybercrimes are characterized by different actors, targets and methods;
- public authorities are progressively building a cybersecurity policy;
- this policy still underestimates some key aspects of the fight against cybercrime.

Sommaire

Introduction

L'Afrique est considérée comme « l'océan bleu numérique du monde, c'est-à-dire un de ces grands espaces dynamiques encore dans une phase d'émergence [1] ». La téléphonie mobile est sans conteste le levier de l'appropriation du numérique en Afrique et c'est sur cette base qu'ont été créées les différentes plateformes et applications de la FinTech africaine[2]. Cependant, en termes d'appropriation du numérique, l'Afrique n'est pas un tout homogène et l'Afrique centrale accuse un retard par rapport à d'autres régions du continent[3].

Chiffres d'utilisation d'internet en Afrique centrale

Source : « Les chiffres d'utilisation d'internet en Afrique centrale (janvier 2023) », Agence Ecofin, 21 août 2023, disponible sur : www.agenceecofin.com.

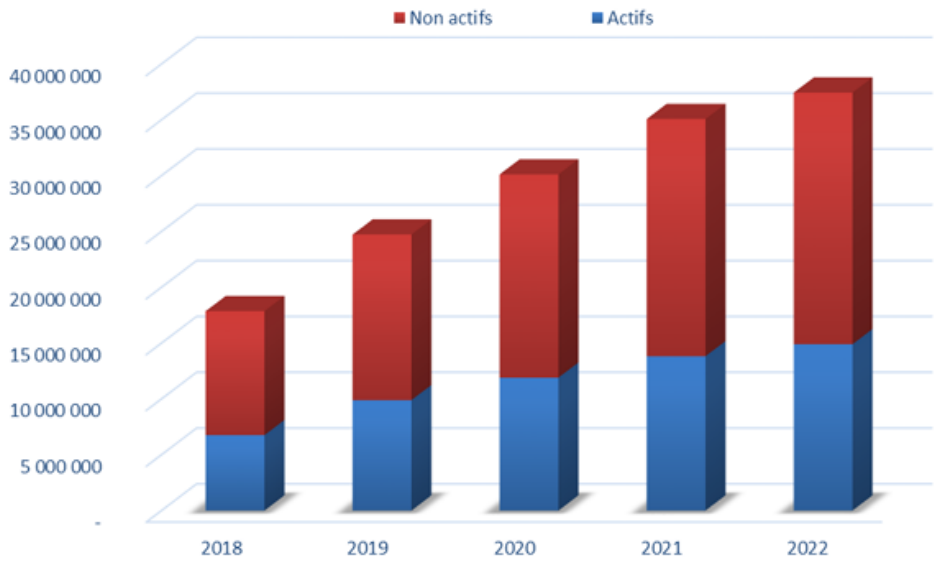
Bien qu'encore à leurs débuts, les paiements numériques connaissent une croissance dynamique en Afrique centrale avec 264 start-ups de commerce électronique [4] et un marché du *mobile money* partagé par 17 opérateurs représentant 14,8 millions de comptes actifs en 2022[5].

---

1. « Développement de l'économie numérique en Afrique : fondements, défis et perspectives », *Jeune Afrique*, disponible sur : www.jeuneafrique.com.
2. A. Kiyindou, « Numérique et technologies financières en Afrique », *in* S. Chauvin, H. Djoufelkit et C. Valadier (dir.), *L'Économie africaine 2023*, Paris, La Découverte, 2023, p. 95-108.
3. « Les chiffres d'utilisation d'Internet en Afrique centrale (janvier 2023) », Agence Ecofin, 21 août 2023.
4. « La CEA et la GSMA appellent l'Afrique centrale à tirer parti de la connectivité mobile pour intensifier le commerce électronique », Commission économique pour l'Afrique, 15 juillet 2021.
5. « Rapport sur les services de paiement dans la CEMAC en 2022 », Banque des États de l'Afrique centrale (BEAC), 2023.

Ce marché est en constante évolution depuis 2018 (cf. graphique ci-dessous [6]). Les prestataires de services de paiement électronique au Cameroun réalisent 69,14 % des transactions de la Communauté économique et monétaire d'Afrique centrale (CEMAC), suivis par le Congo (18,47 %) et le Gabon (11,38 %)[7].

Nombre d'utilisateurs de monnaie électronique dans la CEMAC



Source : « Rapport sur les services de paiement dans la CEMAC en 2022 », Banque des Etats de l'Afrique centrale (BEAC), 2023.

Le développement rapide de la téléphonie mobile en Afrique centrale a pour contrepartie un développement tout aussi rapide de la cybercriminalité. De ce fait, cette étude identifie les formes les plus courantes de la cybercriminalité en Afrique centrale, le profil des cybercriminels et de leurs victimes ainsi que les divers modes opératoires. À l'aune de ces informations, la seconde partie de cette étude analyse les politiques de lutte contre la cybercriminalité en Afrique centrale. L'arrière-plan théorique de ce travail est la problématique de l'adaptation des politiques publiques de sécurité face à des menaces sécuritaires en constante mutation[8]. Cette *Note* recourt à plusieurs notions familières aux professionnels du numérique mais qui ne le sont pas nécessairement pour les profanes. Leur définition éclairera donc utilement le lecteur.

6. E. K. Kamgang Kenmoe, « Comment aligner le mobile money aux standards des services bancaires classiques en zone CEMAC ? », Portail FinDev, 23 janvier 2024.
7. « Rapport sur les services de paiement dans la CEMAC en 2022 », *op. cit.*
8. C. Hoeffler, C. Ledoux et P. Prat, « Changement », *in* L. Boussaguet, S. Jacquot et P. Ravinet (dir.), *Dictionnaire des politiques publiques*, Paris, Presses de Sciences Po, 2019 [4e édition], p. 132-140.

Définitions préliminaires

Cybercriminalité

Elle désigne toutes les activités criminelles qui ont cours dans le cyberespace et mobilisent internet[9]. « Par extension, elle intègre toute forme de malveillance électronique effectuée à l'aide des technologies informatique et de télécommunication (téléphonie, cartes à puces…) [10] ». La convention de Budapest la définit comme « l'ensemble des infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques, infractions informatiques, infractions se rapportant au contenu et les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes[11] ».

Cyberharcèlement

Il désigne un harcèlement (chantage, insultes, humiliations, rumeurs) effectué grâce à internet, notamment sur des réseaux sociaux ou toute autre plateforme en ligne[12]. Ce harcèlement peut prendre plusieurs formes allant du harcèlement sexuel au harcèlement moral en passant par le harcèlement scolaire[13].

Adresse IP (*Internet Protocol Address*)

Il s'agit du numéro d'identification attribué à tout appareil connecté à internet[14]. Il faut noter qu'il existe aujourd'hui des techniques soit pour la cacher, soit pour la rendre variable et empêcher toute traçabilité.

***Malware* ou logiciel malveillant**

« Il existe un très grand nombre de logiciels malveillants, le ver informatique, le virus, le cheval de Troie en sont des exemples. Ils ont pour but d'infiltrer un ordinateur ou un réseau afin d'entraver son bon fonctionnement ou d'en prendre le contrôle[15]. »

Cyber attaque

Il s'agit de vol, d'exposition, d'altération, de désactivation ou de destruction des biens d'autrui *via* un accès non autorisé à des systèmes informatiques[16].

9. S. Ghernaouti et A. Dufour, « Cybercriminalité et cybersécurité », *in* S. Ghernaouti et A. Dufour (dir.), *Internet*, Paris, Presses Universitaires de France, 2012 [11e édition], p. 94-108.
10. *Ibid.*
11. Convention sur la cybercriminalité, publiée par le décret n° 185 du 23 novembre 2001, disponible sur : www.coe.int.
12. « 15 minutes pour comprendre le cyberharcèlement », UNICEF France, mars 2019.
13. « Cyberharcèlement (harcèlement sur internet) », Service Public, 31 octobre 2025.
14. A. Desforges et E. Déterville, « Lexique sur le cyberespace », *Hérodote*, n° 152-153, 2014/1-2, 2014, p. 22-25.
15. *Ibid.*
16. T. Krantz et A. Jonker, « Qu'est-ce qu'une cyberattaque ? », IBM, disponible sur : www.ibm.com.

Mobile money

Cette expression désigne un service qui permet aux personnes disposant d'un mobile de faire des transactions financières *via* un porte-monnaie électronique qui se substitue au compte bancaire. En fonction de la qualité du terminal, on peut directement taper des codes sur le clavier pour faire des transactions ou alors faire usage d'une application pour les téléphones les plus récents[17].

Méthodologie

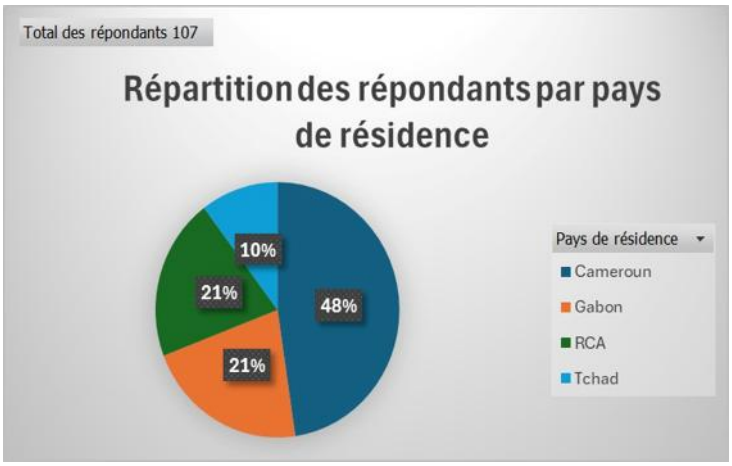
Cette *Note* repose sur une recherche conduite entre octobre 2024 et mars 2025 basée sur une revue de la documentation en source ouverte (médias, rapports, livres, etc.), un sondage en ligne et des entretiens directs et à distance. Un sondage sur un échantillon de 107 personnes au Cameroun, en Centrafrique, au Gabon et au Tchad a permis de récolter des données empiriques relatives aux formes et techniques de cybercriminalité, aux auteurs et victimes de ces actes et à la lutte contre la cybercriminalité. Un questionnaire en ligne a porté principalement sur :

- la connaissance et l'expérience de la cybercriminalité ;
- la lutte contre la cybercriminalité.

La plupart des sondés étaient des Camerounais, suivis des Gabonais, des Centrafricains et des Tchadiens[18]. Les graphiques ci-dessous indiquent la répartition par pays de résidence, par âges et genres des sondés. On peut noter que la répartition par tranche d'âge reflète l'usage des services numériques selon les générations.

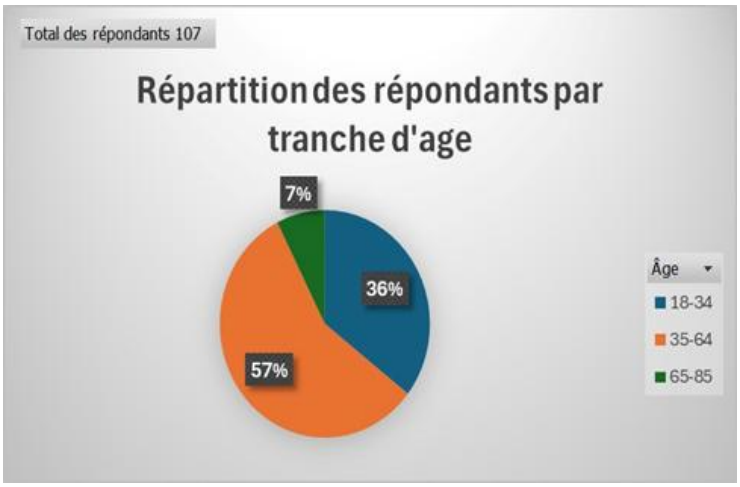
17. A. Martah et F. Gire, « Le *mobile money* : une alternative au compte bancaire pour les petites entreprises au Sénégal ? », Hello Future Orange, 3 décembre 2024, disponible sur : https://hellofuture.orange.com.
18. Données compilées par l'auteur.

Répartition des répondants par pays de résidence



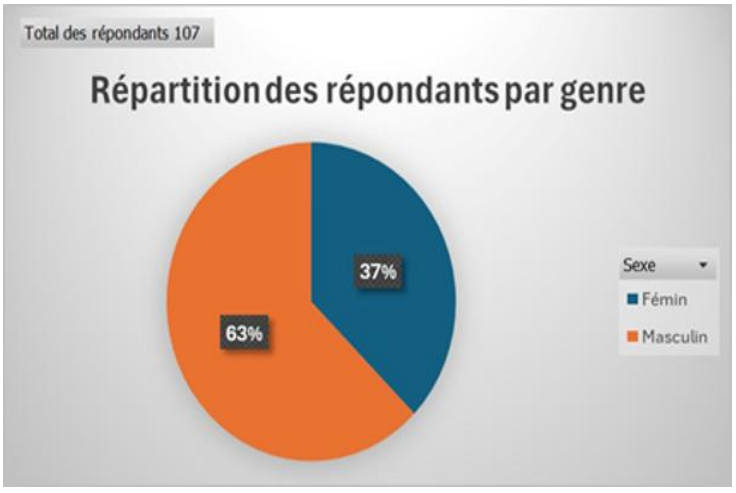
Source : Auteur.

Répartition des répondants par tranche d'âge



Source : Auteur.

Répartition des répondants par genre



Source : Auteur.

Il ressort que, sur l'échantillon escompté, il y a eu un fort taux d'absence de réponses en raison du sentiment anti-français. Informés que le sondage était effectué pour un organisme de recherche français, beaucoup ont refusé de répondre, notamment en Centrafrique, au Gabon et au Tchad. Au Cameroun, les officiels sollicités pour cette analyse ont été plus réticents que les citoyens ordinaires. Pour l'ensemble des pays, beaucoup d'officiels ont souhaité s'exprimer anonymement et d'autres ont simplement décliné. En outre, plus d'une vingtaine de personnes ont été interviewées en présentiel (au Cameroun) ou à distance, *via* WhatsApp au Tchad, en Centrafrique, au Gabon et au Cameroun.

Panorama de la cybercriminalité en Afrique centrale

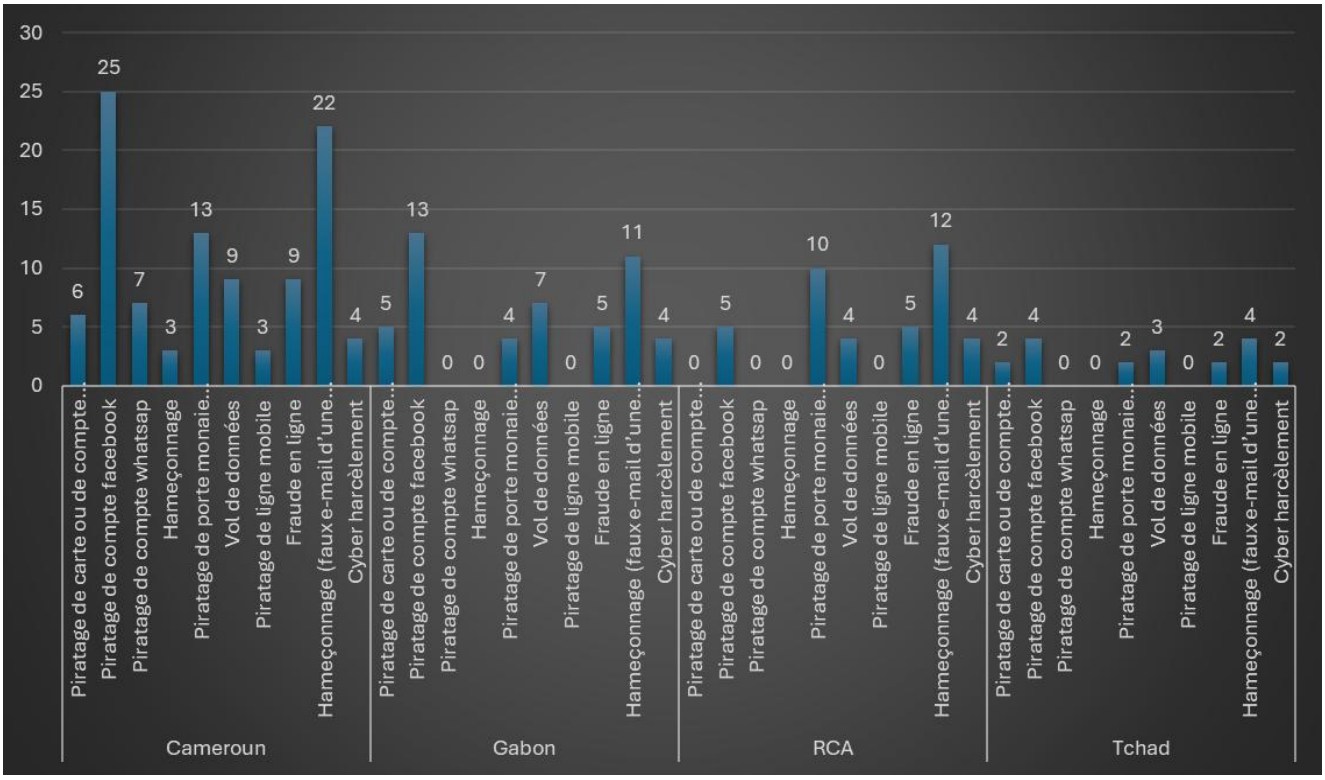
Si en Afrique centrale, comme ailleurs, la cybercriminalité recouvre une grande variété d'activités dont la typologie est forcément incomplète, on peut cependant distinguer quelques grandes catégories d'infractions numériques et en analyser les modes opératoires. La recherche empirique permet également de dresser les profils des cybercriminels et de leurs cibles.

Typologie de la cybercriminalité en Afrique centrale

L'ampleur de la cybercriminalité en Afrique centrale est importante. En effet, sur 107 répondants, 90 % reconnaissent avoir été victimes d'actes cybercriminels, ce qui concorde avec le rapport d'INTERPOL sur l'évaluation des cybermenaces en Afrique[19]. Les formes que prend la cybercriminalité dans les pays de l'étude sont très similaires. Les principales infractions sont par ordre décroissant le piratage de compte, l'hameçonnage, le vol de porte-monnaie électronique et le harcèlement. Facebook et WhatsApp étant les réseaux sociaux les plus utilisés, ce sont surtout ces comptes qui sont piratés. Les exemples ci-dessous sont issus des entretiens avec des victimes de la cybercriminalité ordinaire et illustrent les principales catégories d'infractions numériques.

19. Le premier rapport d'INTERPOL sur la cybercriminalité date de 2021. Le dernier rapport de 2024 est donc la troisième édition : « Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique – Perspectives du bureau pour les opérations de lutte contre la cybercriminalité en Afrique », INTERPOL, 3ème édition, avril 2024, disponible sur : www.interpol.int. Outre les rapports annuels d'INTERPOL, sur l'évaluation de la cybercriminalité en Afrique, on lira avec intérêt : N. Allen, M. La Lime et T. Samme-Nlar, « The Downsides of Digital Revolution – Confronting Africa's Evolving Cyber Threats », Global Initiative Against Transnational Organized Crime, décembre 2022, disponible sur : https://globalinitiative.net et « Cyber Crime & Cyber Security – Trends in Africa », Africa Union Commission (AUC) et Symantec, novembre 2016, disponible sur : https://securitydelta.nl.

Répartition des types d'actes cybercriminels par pays



Source : Auteur.

Le piratage de compte de réseaux sociaux

La transmission de liens frauduleux après la mise en confiance des utilisateurs conduit souvent au piratage de comptes WhatsApp, Facebook et mail. À titre d'exemples relevés lors des entretiens, une utilisatrice qui a reçu des mails avec de fausses adresses et de faux liens a cliqué sans savoir quelles pouvaient être les conséquences. Immédiatement, ses contacts ont reçu des messages de demande d'argent et son compte WhatsApp a été piraté. Déconnectée pendant quelques jours, elle a ensuite reçu des messages de personnes réclamant leur argent pour une soi-disant offre qu'elle leur aurait proposée[20].

L'hameçonnage

Ce cybercrime qui consiste à utiliser de faux courriels, sites Web et messages textes incitant la victime à révéler des informations personnelles et corporatives confidentielles (données de carte de crédit, numéro de téléphone, adresse postale, informations sur une entreprise, etc.) est fréquent.

20. Entretien réalisé le 16 décembre 2024 en ligne avec une victime au Cameroun.

Ainsi, lors de l'achat d'un PC en ligne sur un site de vente entre particuliers, un de nos sondés au Gabon a fait l'objet de ce genre d'arnaque. L'acheteur voulait faire un paiement en ligne mais le site apparemment ne fonctionnait pas. Cependant, le lendemain, il a reçu un message de débit de sa carte bancaire alors qu'il n'avait initié aucune action dans ce sens. Le site de vente était en fait un doublon et les informations bancaires envoyées étaient récupérées pour être utilisées frauduleusement[21].

Le vol de porte-monnaie électronique

Il s'agit là aussi d'un cybercrime très répandu. Au Cameroun, lors de l'achat d'un billet de bus de voyage en ligne, un de nos enquêtés est tombé malencontreusement sur un site frauduleux. Après la tentative infructueuse d'achat de billet, il a reçu un appel d'une soi-disant employée de l'agence de bus. Elle lui a indiqué alors qu'elle avait constaté qu'il avait des difficultés pour acheter son billet et lui a demandé ses données de compte *mobile money* MTN MoMo pour réaliser l'opération. C'est ainsi que son compte *mobile money* a été vidé[22]. De même, de faux employés de la compagnie de téléphonie mobile Airtel Gabon ayant mis en place un service de *mobile money* contactaient les usagers pour leur soutirer des informations afin de vider leurs comptes[23].

Le cyberharcèlement

Lors de notre enquête, plusieurs femmes ont déclaré avoir été victimes de cyberharcèlement. Il s'agit de cyberharcèlement avec ou sans chantage financier basé sur des photos ou des vidéos intimes. Dans certains cas, ces photos ou vidéos ont été obtenues par le vol. Récemment, une cadre de l'hôpital général de Douala au Cameroun a fait l'objet d'une tentative de chantage après qu'une personne du service informatique a eu accès à son téléphone pour le réparer et lui a dérobé des vidéos intimes[24]. Mais, dans d'autres cas, les vidéos ou photos ont été envoyées dans le cadre d'une relation sentimentale qui a mal tourné. L'amoureux déçu ou éconduit tente de se venger en dévoilant des photos intimes de son ex-compagne ou maîtresse (« *revenge porn* »). De l'avis de certains enquêtés, la difficulté de ces situations peut mener les victimes à envisager le suicide[25]. Les victimes de cette pratique ont souvent trop honte pour porter plainte.

21. Entretien réalisé le 18 décembre 2024 en ligne avec une victime en Centrafrique.
22. Entretien réalisé le 5 décembre 2024 à Yaoundé avec une résidente de la ville de Douala.
23. « L'opérateur Airtel Gabon enquête sur les attaques de son service Mobile money », *Le Nouveau Gabon,* 20 août 2021.
24. « Paul Chouta donne des détails sur les sextapes de Chantal », CamerounWeb, 10 mars 2025.
25. Entretien mené à Yaoundé le 18 décembre 2024 avec une étudiante de l'Université de Yaoundé I.

Les exemples collectés lors de cette recherche ne suffisent pas à dresser un panorama exhaustif des techniques cybercriminelles mais ils mettent en évidence l'ingéniosité créative des cybercriminels. Dans ce domaine, l'imagination est sans limite et les cybercriminels recourent à une gamme de ruses allant des plus simples aux plus sophistiquées. Ces ruses vont de l'exploitation de la négligence des usagers (des internautes laissent leurs données personnelles accessibles en oubliant de se déconnecter dans les cybercafés par exemple) au clonage de sites web ou d'applications.

La variété des escroqueries en ligne est très vaste et elles combinent le plus souvent à la fois la manipulation psychologique et l'intrusion numérique. Outre le classique *spamming*[26], on trouve des propositions d'investissement alléchantes ou de fausses annonces immobilières diffusées sur les réseaux sociaux afin de réaliser des arnaques relativement classiques[27]. Il y a aussi des escroqueries aux faux ordres de virement[28], de faux sites d'entreprises qui permettent de faire des paiements numériques ou de faux sites administratifs qui permettent de collecter des données financières ou administratives personnelles[29]. Le clonage des sites web nécessite d'être attentif et expérimenté pour l'identifier[30]. Les différences entre la charte graphique du site frauduleux et le site original sont souvent difficiles à déceler. En tout état de cause, l'usager n'a pas suffisamment de temps pour y prêter attention et peut même être pressé d'agir par un coup de fil stressant. La clé des cyber-arnaques est évidemment la mise en confiance de la victime grâce à l'imitation des sites web et/ou à l'observation rigoureuse des habitudes des internautes. Cette mise en confiance de la victime s'effectue parfois sur le long terme et cette manipulation psychologique conduit souvent à la transmission des liens frauduleux pour réaliser des piratages de comptes[31].

Les exemples de cybercriminalité révélés par le sondage mettent en évidence les outils des auteurs d'actes cybercriminels : virus informatiques, logiciels malveillants (zombies ou *botnets* qui espionnent et utilisent les machines de leurs victimes, chevaux de Troie bancaires) et rançongiciels (logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers).

26. Envoi de messages à des milliers de destinataires proposant généralement une offre financière alléchante.
27. L. Ntoutoume, « Fausses annonces immobilières : Des réseaux d'arnaque s'installent sur Facebook », *GabonReview*, 1er décembre 2020.
28. Les cybercriminels piratent ou imitent des comptes professionnels et incitent des employés à procéder à des transferts de fonds non autorisés.
29. Deux cas au Cameroun et au Gabon : E. Djene, « Un jeune cybercriminel de 21 ans spécialisé dans les extorsions en ligne arrêté à Yaoundé », *Actu Cameroun*, 13 avril 2024, disponible sur : https://actucameroun.com et « Le gouvernement met en garde contre un faux site de distribution d'aides sociales au Gabon », *Le Nouveau Gabon*, 23 juillet 2021, disponible sur : www.lenouveaugabon.com.
30. G. Sylvestre, « De bons réflexes pour éviter les risques de phishing/ransomware », *I2D – Information, données & documents*, vol. 54, n° 3, 2017, p. 44-46.
31. J. Tilouine et O. Dumons, « Les nouvelles "cyberarnaques" africaines », *Le Monde*, 9 mars 2017.

D'un point de vue technique, cela dénote un niveau de sophistication relativement élevé[32].

Criminels et victimes

Le profil des cybercriminels

Les cybercriminels ont des profils variés qu'on peut cependant classer en deux grandes catégories, à savoir les professionnels et les amateurs.

Les cybercriminels occasionnels

Il s'agit d'opportunistes qui se retrouvent par hasard en présence d'un appareil ou de données qu'ils vont utiliser pour commettre des actes relevant de la cybercriminalité. La gamme d'individus concernés est très variée à tel point qu'on pourrait dire qu'il n'y a pas de profil spécifique. Parmi les cas mentionnés lors de cette recherche, on peut citer un chauffeur de taxi qui a profité du téléphone portable oublié par un de ses clients dans son véhicule. Il a contacté certains proches de son passager dont les numéros se trouvaient dans le répertoire. Il leur a déclaré avoir trouvé le téléphone par hasard et qu'il souhaitait le remettre au propriétaire contre une récompense. Ne recevant pas de réponse, le taximan a rappelé pour indiquer qu'il s'impatientait et qu'il allait publier des vidéos intimes du propriétaire trouvées sur ce téléphone. Alertés, les services de police ont localisé le téléphone et interpellé le chauffeur de taxi[33]. Certaines personnes peuvent aussi recevoir des vidéos ou photos intimes sans les avoir recherchées et peuvent décider de les monnayer. C'est ainsi le cas d'une vidéo issue d'un groupe de libertinage à Bangui qui a été communiquée à plusieurs personnes. Après avoir reconnu la jeune femme de la vidéo, un jeune homme l'a contactée et a exigé une somme pour supprimer la vidéo[34].

Les cybercriminels professionnels

À l'inverse des cybercriminels occasionnels, les professionnels de la cybercriminalité ne sont pas toujours des citoyens des pays d'Afrique centrale. La nature mondiale des réseaux décorrèle la nationalité et la criminalité. De même, à l'inverse des cybercriminels opportunistes, les professionnels analysent l'environnement ou les cibles qu'ils souhaitent attaquer, identifient des habitudes et des failles (techniques ou humaines).

32. « La cybercriminalité », Agence nationale des technologies, de l'information et de la communication (ANTIC), disponible sur : www.antic.cm.
33. Entretien réalisé au Gabon en ligne le 14 décembre 2024.
34. Entretien réalisé en République centrafricaine (RCA) en ligne avec un web-activiste le 16 décembre 2024.

Pour mener leur attaque, ils vont parfois utiliser des programmes informatiques et fabriquer des liens frauduleux.

Au Cameroun, les spécialistes de l'arnaque en ligne se trouvent principalement dans les villes de Buea, Yaoundé, Douala, Bamenda et Bafoussam. D'après les forces de sécurité, ils « ont généralement des locks, de gros bijoux, plusieurs téléphones, de grosses motos, des véhicules chers et fréquentent généralement les snacks et boites de nuit, y compris les jours qui ne sont pas habituels pour ces milieux-là, par exemple le lundi[35] ». Ils ont également plusieurs ordinateurs portables et changent constamment de puces téléphoniques pour commettre leur forfait. Surtout, ils disposent d'un petit téléphone appelé « *tchoronko* » qui est difficile à localiser en cas d'enquête[36], non pas parce que le téléphone n'est pas localisable, mais parce qu'avec un Android ou un Iphone par exemple, la dernière connexion suffit pour localiser le téléphone à partir de l'adresse IP. Une opération de police de routine a permis de découvrir à Yaoundé que certains déplacés de la crise anglophone étaient en fait des hackers. Ces derniers disposaient de vieux ordinateurs et téléphones portables avec lesquels ils opéraient[37].

Ces spécialistes de l'arnaque en ligne peuvent aussi agir depuis des prisons, comme au Gabon où des prisonniers montent des opérations d'extorsion de fonds avec des téléphones portables[38]. Bien que les autorités policières des pays de la sous-région peinent à le reconnaître, certains cybercriminels professionnels agissent aussi dans le champ politique. Ces cyber-mercenaires attaquent les comptes en ligne de politiciens pour le compte d'autres politiciens[39].

Le profil des victimes

Les victimes de la cybercriminalité en Afrique centrale peuvent se catégoriser en trois groupes.

L'usager quotidien

Comme le montrent les exemples précédemment cités issus de cette recherche, les citoyens ordinaires sont victimes de la cybercriminalité en raison de la généralisation de la téléphonie mobile, du *mobile money* et des réseaux sociaux, par lesquels les cybercriminels africains contactent souvent leurs cibles. Les franges les plus modestes de la population qui sont non bancarisées recourent de plus en plus au *mobile money* et sont donc

35. Entretien mené à Yaoundé avec un membre des forces de sécurité en janvier 2025.
36. *Ibid.*
37. Entretien mené à Yaoundé avec un acteur judiciaire en février 2025.
38. Entretien mené en ligne au Gabon le 12 novembre 2024.
39. M. Bobbo et T. Vircoulon, « Politique et réseaux sociaux : influenceurs et bloggeurs dans le jeu politique camerounais », *Notes de l'Ifri*, Ifri, décembre 2024.

souvent victimes des arnaques liées à ce moyen de paiement. De même, le cyberharcèlement spécifique cible les femmes.

Les membres de l'élite

La cybercriminalité concerne tout le monde, mais l'élite politico-économique est particulièrement ciblée en raison de ses ressources. Au Cameroun, plusieurs affaires de cybercriminalité ont affecté des personnalités de l'*establishment* politique. En janvier 2025, le ministre des Finances du Cameroun tirait la sonnette d'alarme au sujet des faux comptes qui existent sur LinkedIn en son nom : « Certains de ces comptes usurpateurs publient des informations officielles pour paraître plus crédibles, et certains ont même accumulé une centaine d'abonnés[40]. »

Dans le même ordre d'idées, lorsque la Direction générale des services spéciaux du Gabon a démantelé un réseau d'escroquerie téléphonique, elle s'est rendu compte que le Premier ministre par intérim, Raymond Ndong Sima, était l'une des cibles[41]. Au Cameroun, on dénombrait déjà, dans la deuxième moitié des années 2010, 156 faux comptes Facebook des personnalités publiques[42].

Les organismes publics et le secteur privé

Les intrusions dans les systèmes des organismes publics et des entreprises en Afrique centrale ne sont pas nouvelles. Il y a 15 ans, des sites web d'administrations, d'universités et de médias étaient piratés au Cameroun. De même, des entreprises publiques et privées (Camair-Co, Ecobank, BICEC) étaient déjà victimes de fraudes informatiques[43]. De nombreuses attaques récentes montrent que les organismes publics[44] et les entreprises sont toujours aussi menacés. En septembre 2024, deux agents de la Caisse nationale de prévoyance sociale au Cameroun auraient cliqué sur un lien malveillant qui a permis aux cybercriminels d'accéder aux bases de données, puis d'exiger des rançons[45]. En 2023, le site web du Trésor public

40. « Attention, de faux comptes au nom du ministre des Finances circulent sur les réseaux sociaux », Stopblablacam, 24 janvier 2025.
41. « [INTERVIEW – DIDIER SIMBA] Le 1er ministre gabonais ciblé par une cyberattaque : Les conséquences », chaîne YouTube *Didier SIMBA*, 26 février 2025, disponible sur : www.youtube.com.
42. A. Assako, « Niveaux de responsabilités en cybersécurité et lutte contre la cybercriminalité », *in* « Actes du séminaire de recherche sur : "Les défis et enjeux de la cyber-criminalité et la cyber-sécurité en Afrique centrale" », *VIGIE – Bulletin d'analyses stratégiques et prospectives*, École supérieure internationale des forces de sécurité, décembre 2018, disponible sur : www.eiforces.gov.cm.
43. B. Djamen, « Web space : sommes-nous en sécurité ? », Gefona Digital Foundation, 12 mai 2020.
44. En 2023, l'Union africaine a été la cible d'une cyberattaque menée par le groupe BlackCat. Voir : « Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique », *op. cit.*
45. « La CNPS confirme le piratage de ses données informatiques par des hackers », CamerounWeb, 30 septembre 2025.

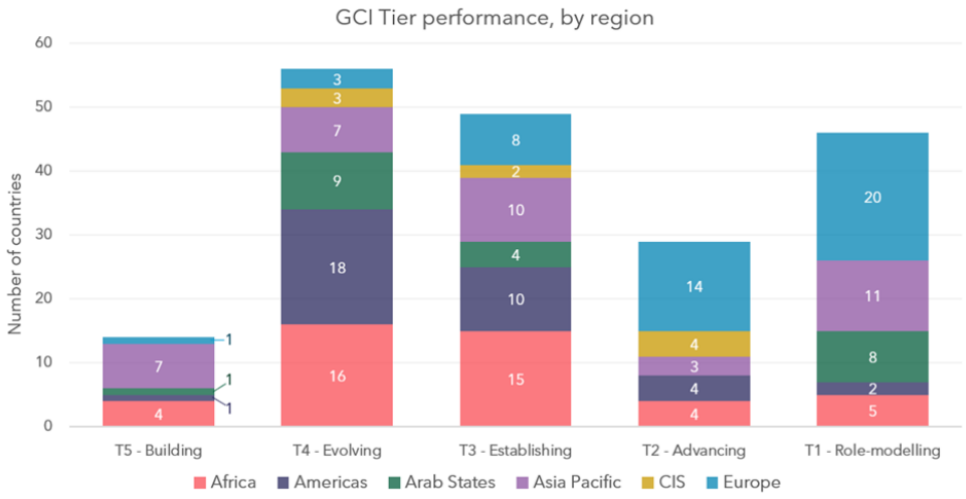
gabonais a aussi été piraté[46]. Le secteur bancaire est l'une des cibles privilégiées des cybercriminels, comme l'a souligné en 2021 le comité de stabilité financière d'Afrique centrale présidé par le gouverneur de la Banque des États d'Afrique centrale (BEAC)[47]. Ainsi au Gabon, plusieurs banques ont fait l'objet de cyberattaques[48]. En 2020, des hackers localisés au Mexique ont effectué des retraits frauduleux à la Banque internationale pour le commerce et l'industrie du Gabon (BICIG)[49]. De même, une importante attaque contre la BGFIBank a été menée en juin 2023 par le groupe cybercriminel BianLian. Cette attaque a permis d'accéder à des fichiers importants qui exposaient la banque. « Les cybercriminels ont exigé une rançon de 55 bitcoins, équivalant à environ 1,5 million d'euros ou 998 millions de FCFA [franc CFA][50] ». Au début de cette année, le site web de la BEAC a été temporairement bloqué par le collectif de hackers bien connu, Anonymous Sudan[51].

46. « Cyberattaque d'ampleur à la CNPS Cameroun : des millions de données compromises, les hackers exigent une rançon », Econuma, 13 septembre 2024.
47. « Communiqué de presse », Comité de stabilité financière d'Afrique centrale, 29 novembre 2021.
48. L. Ntoutoume, « Cybercriminalité : OPERA1ER a volé environ 11 millions de dollars au Gabon et dans 14 autres États », *GabonReview*, 10 novembre 2022.
49. I. El Yadari, « Cyberattaque : des milliers d'euros dérobés à une filiale gabonaise de la BCP », Le Desk, 18 mai 2020.
50. K. Acakpo, « Cyberattaque contre la BGFIBank : la liste des fichiers volés désormais en accès sur internet », *Africa CyberSecurity Magazine*, 26 juin 2023.
51. C. Houeto, « Anonymous Sudan revendique une cyberattaque sur la Banque Centrale des États de l'Afrique Centrale », *Africa CyberSecurity Magazine*, 10 janvier 2025.

Les politiques de lutte contre la cybercriminalité en Afrique centrale

Face à l'expansion de la cybercriminalité en Afrique centrale, depuis quelques années, les dirigeants des pays de cette région ont multiplié les initiatives pour construire une politique de cybersécurité. Toutefois, ces initiatives sont encore trop partielles et les pays de la sous-région sont mal classés selon l'indice de la cybersécurité de l'Union internationale des télécommunications[52].

Répartition par région à travers cinq niveaux (tiers) de maturité en cybersécurité



Source : « Global Cybersecurity Index 2024 », 5e édition, International Telecommunication Union, 2024.

52. « Global Cybersecurity Index 2024 », 5e édition, International Telecommunication Union, 2024, disponible sur : www.itu.int.

La réponse des pouvoirs publics

Encadrement normatif et administratif

Les gouvernements de la sous-région ont adopté des cadres juridiques définissant la cybercriminalité, instaurant un régime de sanctions, déterminant des obligations de cybersécurité et créant des agences de supervision. Dans la sous-région, les deux derniers pays à adopter une telle législation sont la Centrafrique (2024) et le Gabon (2023)[53].

Les textes législatifs sur la cybercriminalité en Afrique centrale définissent clairement les actes qui peuvent être considérés comme des actes cybercriminels : la piraterie informatique, la fraude électronique, le vol des données personnelles, les accès illicites, les attaques actives, l'atteinte à l'intégrité, les contenus illicites, le déni d'accès de service, l'interception illégale, l'intrusion par intérêt… Ces textes définissent également les critères pour déterminer si un acte constitue une infraction cybercriminelle, comme l'intention de nuire, la nature de l'acte et les conséquences pour les victimes[54]. Ils prévoient aussi de nouvelles possibilités d'investigation telles que l'interception des communications électroniques et des données électroniques. Ainsi l'article 37 de la loi tchadienne sur la lutte contre la cybercriminalité confère au procureur de la République la possibilité d'« utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu des communications spécifiques, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, avec les moyens techniques existants, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatiques[55] ».

Les textes juridiques sur la cybercriminalité en Afrique centrale accordent une attention particulière à la protection des droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi qu'aux intérêts légitimes des personnes morales[56]. En effet, les lois et règlements en vigueur contiennent des dispositions spécifiques pour protéger les données

53. G. Ondo Nzuey, « Cybercriminalité : le Gabon veut adapter son dispositif sécuritaire au phénomène », *GabonReview*, 25 mai 2023.
54. Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun.
55. Loi n° 009/PR/2015 du 10 février 2015 portant sur la cybersécurité et la lutte contre la cybercriminalité au Tchad.
56. Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun ; loi n°009/PR/2015 du 10 février 2015 portant sur la cybersécurité et la lutte contre la cybercriminalité au Tchad, chapitre II/section I et l'ordonnance n° 15/PR/2018 du 23 février 2018 portant sur la réglementation de la cybersécurité et la lutte contre la cybercriminalité en République gabonaise (son article 2 fait un point sur la protection de la vie privée des populations).

personnelles et les informations sensibles des individus, ainsi que pour prévenir les atteintes à leur honneur et à leur réputation[57]. Par ailleurs, les textes juridiques protègent également les intérêts légitimes des personnes morales (les entreprises et les organisations) avec des dispositions relatives à leurs secrets et leurs intérêts économiques[58]. Les textes juridiques prévoient la mise en place d'un dispositif de suivi et de régulation des activités de sécurité électronique chargé de superviser les activités des fournisseurs de services de sécurité électronique, ainsi que des normes pour la sécurité des systèmes d'information[59]. En effet, les lois et règlements en vigueur exigent que les fournisseurs de services de communication électronique mettent en place des mesures de sécurité pour protéger les données personnelles et les communications des utilisateurs[60]. Les autorités de régulation sont chargées de certifier les systèmes de sécurité mis en place par les fournisseurs de services, afin de garantir leur conformité aux normes de sécurité. Par ailleurs, les pays concernés ont établi des autorités de supervision et de régulation[61].

En matière de répression pénale, les textes juridiques proposent un régime de sanctions et de peines robustes pour les infractions liées à la cybercriminalité, incluant des peines d'emprisonnement et des amendes sévères, afin de dissuader les auteurs de ces infractions. La loi du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun prévoit des peines graduées en fonction de la gravité des actes cybercriminels. Le même dispositif est prévu par la réglementation au Gabon[62]. À titre d'exemple, la loi sur la cybersécurité et la lutte contre la cybercriminalité au Tchad dispose qu'« en cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction saisie peut prononcer à titre de peines complémentaires l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction, en couper l'accès par tous moyens techniques disponibles ou même en interdire[63] ». Selon l'article 39 de cette loi, les cybercriminels condamnés doivent diffuser eux-mêmes leur condamnation

57. Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun, chapitre IX, section IV.
58. *Ibid.*
59. Voir la loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun, titre II, chapitre II et la loi n°009/PR/2015 du 10 février 2015 portant sur la cybersécurité et la lutte contre la cybercriminalité au Tchad, titre II, chapitre II.
60. Le dispositif législatif sur la cybersécurité et la lutte contre la cybercriminalité dans les États d'Afrique centrale offrent un cadre propice pour les activités de certification. Voir par exemple l'ordonnance n° 15/PR/2018 du 23 février 2018 portant sur la réglementation de la cybersécurité et la lutte contre la cybercriminalité en République gabonaise, titre II, chapitre III.
61. Voir tableau.
62. Voir par exemple les articles 39 à 72 de l'ordonnance n°15/PR/2018 du 23 février 2018 portant sur la réglementation de la cybercriminalité en République Gabonaise.
63. Loi n°009/PR/2015 du 10 février 2015 portant sur la cybersécurité et la lutte contre la cybercriminalité au Tchad, article 38.

par le même canal utilisé pour commettre l'acte délictueux, faute de quoi la peine sera doublée. En outre, une attention particulière est accordée à la protection des droits des victimes et des témoins de la cybercriminalité, en prévoyant des dispositions pour leur protection et leur soutien. Cela comprend la mise en place de mécanismes de compensation pour les victimes, ainsi que la protection de leur identité et de leur vie privée, le cas échéant.

Les textes juridiques rendent possible la coopération internationale en matière de lutte contre la cybercriminalité, en vue de renforcer la sécurité et la confiance dans l'environnement numérique mondial. Cela inclut les mécanismes d'entraide judiciaire internationale prévus par exemple au chapitre II du titre IV de la loi de 2010 sur la cybersécurité et la cybercriminalité au Cameroun[64] et dans le titre V de la loi similaire au Tchad[65]. Cependant, les États d'Afrique centrale restent peu engagés par les conventions régionales et mondiales relatives à la cybersécurité. Dans la sous-région, seul le Cameroun est signataire de la convention de Budapest adoptée en 2001, qui stipule les lignes directrices pour les pays souhaitant élaborer une législation nationale contre la cybercriminalité[66]. En revanche, le Gabon[67], le Cameroun et le Tchad ont adhéré à la convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (la convention de Malabo) dont le but est de « déterminer les règles de sécurité essentielles à la mise en place d'un instrument juridique de l'Union africaine pour les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité[68] ».

64. Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun.
65. Loi n° 009/PR/2015 du 10 février 2015 portant sur la cybersécurité et la lutte contre la cybercriminalité au Tchad.
66. Loi n° 2022/002 du 27 avril 2022 portant sur l'adhésion du Cameroun à la convention de Budapest sur la cybercriminalité, adoptée le 23 novembre 2001 à Budapest (Hongrie).
67. « Convention de Malabo sur la cybersécurité : le Gabon valide le projet de loi sur la ratification », *Africa Cybersecurity Magazine*, 21 octobre 2024, disponible sur : https://cybersecuritymag.africa.
68. Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel adoptée le 27 juin 2014, disponible sur : www.afapdp.org.

Législations et autorités administratives dans le secteur de la cybersécurité

Pays	Législation	Autorité administrative de supervision et de contrôle
Cameroun	Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun (modifiée par la loi du 20 avril 2015)	Agence nationale des technologies de l'information et de la communication
Centrafrique	Loi sur la cybersécurité et la lutte contre la cybercriminalité du 25 janvier 2024	Agence nationale de la cybersécurité
Gabon	Loi n° 027/2023 du 11 juillet 2023 portant sur la réglementation de la cybersécurité et de la lutte contre la cybercriminalité	Agence nationale des infrastructures numériques et des fréquences
Congo-Brazzaville	Loi n° 27-2020 du 5 juin 2020 portant lutte contre la cybercriminalité	Agence de régulation des postes et des communications électroniques
Tchad	Loi n° 009/PR/2015 portant sur la cybersécurité et la lutte contre la cybercriminalité au Tchad	Agence nationale de sécurité informatique et de certification électronique

Limites des réponses des pouvoirs publics

Bien qu'ayant pris conscience des enjeux, les pouvoirs publics des pays concernés ont élaboré des réponses sécuritaires qui présentent certaines limites de nature variée. De ce fait, d'après le classement mondial de la cybersécurité réalisé annuellement par l'Union internationale des télécommunications, les pays de notre étude ont des scores médiocres. Seul le Cameroun figure dans la catégorie 3 (cf. graphique p. 20), celle des pays consolidant leur politique de cybersécurité. Le Tchad, le Congo et le Gabon sont classés parmi les pays en phase de construction de leur politique de cybersécurité tandis que la Centrafrique fait partie des pays en phase de création d'une politique de cybersécurité[69].

69. L'index mondial de la cybersécurité de l'Union internationale des télécommunications est fondé sur 5 critères d'évaluation : réglementation, capacité technique, organisation, sensibilisation, coopération

L'adaptation continue du droit

Le volontarisme des pouvoirs publics se heurte à la rapidité des évolutions technologiques qui n'attendent pas que des solutions juridiques soient élaborées. En Afrique centrale comme ailleurs, les dispositifs législatifs et réglementaires sont, par définition, pris en défaut par les nouvelles méthodes employées par les cybercriminels. Par exemple, les lois sur la cybercriminalité peuvent ne pas couvrir les utilisations malveillantes de l'intelligence artificielle. Cette lacune peut permettre aux cybercriminels de profiter de ces nouvelles méthodes pour commettre des crimes sans être poursuivis, ce qui souligne la nécessité d'une mise à jour urgente du dispositif législatif.

Même quand il y a une évolution des cadres normatifs comme au Cameroun[70], la mise à jour des capacités et compétences du personnel policier et judiciaire prend du temps et est nécessairement en retard par rapport aux développements de la cybercriminalité. Le manque d'adaptation peut donc créer des écarts dans l'appréciation du phénomène, voire dans la gestion des enquêtes. Cela peut aussi impacter la capacité à renforcer la collaboration entre différents pays.

Une coopération internationale insuffisante

Plusieurs affaires ont mis en lumière la nécessaire coopération internationale en termes de lutte contre la cybercriminalité. En 2017, la police fédérale américaine a transmis des informations à la police camerounaise et des suspects ont été arrêtés à Bamenda, Buea, Kumba, Douala et Yaoundé. Les cybercriminels présumés étaient impliqués dans une escroquerie massive à travers les réseaux sociaux. Leurs victimes, principalement des Américains et des Français, auraient été dépouillées de plus de quatre milliards de francs CFA[71]. De même, « du 2 au 6 septembre 2024, l'Agence nationale des infrastructures numériques et des fréquences (ANINF) et l'unité cybercriminalité de la Police nationale gabonaise ont pris part à l'Africa Cyber Surge Operation (ACSO) à Accra. Cette rencontre, destinée à lutter contre la cybercriminalité en Afrique, est à l'initiative d'INTERPOL, d'AFRIPOL et du département d'Investigation criminelle du Ghana[72] ». Toutefois, cette coopération internationale évolutive ne doit pas dissimuler que l'harmonisation des cadres juridiques nationaux est encore

internationale. Les pays sont classés en 5 catégories (la catégorie 5 réunissant les pays les plus performants). Voir le dernier rapport : « Global Cybersecurity Index 2024 », ITU, *op. cit*,

70. S. Tepi, *La cybercriminalité au Cameroun. Enjeux d'une législation en quête d'efficacité*, Paris, L'Harmattan, 2020.

71. « Cameroun : de présumés cybercriminels arrêtés », BBC News, 16 juillet 2017, disponible sur : www.bbc.com.

72. « Lutte contre la cybercriminalité en Afrique : le Gabon classés 3ème sur 25 participants », ANINF, 9 septembre 2024, disponible sur : https://aninf.ga.

insuffisante. En effet, tous les États d'Afrique centrale n'ont pas ratifié la convention de Budapest ni celle de Malabo. À ce jour, si trois États parmi ceux de notre étude sont signataires de la convention de Malabo, seuls deux (le Tchad et le Gabon) l'ont ratifiée[73]. Les délais entre l'adoption de la convention de Malabo et sa ratification ont été longs[74]. Par ailleurs, parmi les pays de notre étude, le Tchad et la Centrafrique n'ont pas participé à l'édition 2024 du rapport d'INTERPOL sur l'évaluation des tendances de la cybercriminalité en Afrique[75].

L'investissement dans les capacités techniques et humaines

La faible qualité de l'accès à internet et les problèmes de fourniture d'électricité représentent des contraintes importantes. Comment mener des investigations sur des outils sophistiqués ou encore réagir à temps lorsqu'un signalement est fait alors que la qualité de l'accès à internet pose des problèmes en Afrique centrale ? Il arrive encore que des utilisateurs n'aient accès qu'à la 3G sur leur téléphone mobile. En outre, les capacités techniques pour la lutte contre la cybercriminalité se heurtent à un problème d'accès à l'énergie. Les coupures d'électricité sont encore fréquentes dans les pays de l'analyse.

Le manque d'investissements dans les cybercapacités des services chargés de lutter contre cette forme de criminalité constitue aussi une autre limite car mener une enquête sur la cybercriminalité nécessite d'avoir un appareillage technique de pointe. Si l'on note que les États fournissent un effort à travers leurs agences nationales de régulation, celui-ci reste encore insuffisant face aux techniques sophistiquées des cybercriminels, notamment pour brouiller les pistes de leurs adresses IP. Cela est encore plus difficile lorsque les cybercriminels agissent à partir de plusieurs pays. En raison de la qualité des équipements utilisés, le spectre du rayon de localisation des téléphones mobiles peut être approximatif[76]. Cette absence de précision peut empêcher de retrouver des cybercriminels. De même, il est parfois impossible de remonter à un identifiant à partir du numéro de la carte nationale d'identité quand on utilise un téléphone enregistré au nom d'une autre personne ou parce qu'une partie de la population dans les pays de cette étude ne dispose pas d'une carte nationale d'identité. L'exploitation des listings téléphoniques dans le cadre des enquêtes cybercriminelles n'est

73. A. Gakiria et T. M. Gitonga, « Qu'est-ce que la convention de Malabo ? », Fondation Diplo, 29 janvier 2025, disponible sur : www-diplomacy-edu.translate.goog.
74. C. Houeto, « Entrée en vigueur de la Convention de Malabo sur la cybersécurité en Afrique : les pays l'ayant ratifiée 9 ans après », *Africa Cybersecurity Magazine*, 5 octobre 2023, disponible sur : https://cybersecuritymag.africa.
75. « Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique », *op. cit.*
76. Entretien mené en ligne en mars 2025 en RCA, au Tchad, au Gabon et au Cameroun avec des acteurs sécuritaires et des web-activistes.

pas toujours aisée[77]. L'un des moyens de contourner cet écueil consiste à se focaliser sur les contacts les plus récurrents (appels et SMS), ainsi que sur les bornes les plus usitées. Cela permet de localiser les endroits régulièrement fréquentés par les présumés cybercriminels et ceux et celles avec qui ils interagissent constamment. Par ailleurs, dans la sous-région, les Computer Emergency Response Teams qui sont « des unités d'experts ayant pour mandat de porter assistance aux individus ou aux institutions qui sont l'objet de cyberattaques [78] » n'existent actuellement qu'au Cameroun. Cette unité est logée au sein de l'Agence nationale des technologies de l'information et de la communication. L'unité est en cours de création au Tchad, au Gabon et en Centrafrique[79].

En définitive, l'investissement continu dans l'amélioration des compétences des personnels des organismes et services chargés de la cybersécurité est une nécessité face à des innovations technologiques permanentes[80]. En termes de formation et d'équipements, le travail et le soutien d'INTERPOL ne sont pas négligeables mais ils doivent être amplifiés[81].

Le silence des victimes

La cybercriminalité est insuffisamment connue et donc mal combattue en raison du silence des victimes. En effet, ces dernières ne portent pas souvent plaintes, voire préfèrent dissimuler leur situation. Cela s'observe très souvent avec les cyberharcèlements. Certaines personnes interviewées ont honte de porter le problème en justice quand il s'agit, par exemple, de questions d'ordre sexuel avec des photos et vidéos suggestives[82]. Mais cela est aussi vrai dans les cas d'intrusions dans les systèmes informatiques d'entreprises. La banque gabonaise BGFI, dont nous avons parlé précédemment, n'a pas communiqué sur l'attaque dont elle avait fait l'objet. C'est un hacker éthique qui a en effet révélé l'affaire en précisant que la banque était restée silencieuse dans le but de protéger son image commerciale[83]. Enfin, le manque de confiance dans l'efficacité des autorités chargées de lutter contre la cybercriminalité joue aussi un rôle préjudiciable. Le silence des victimes accentue le déficit de connaissances sur la cybercriminalité.

77. Entretien réalisé au Tchad en ligne en mars 2025.
78. M. K. Alassane, « Que retenir des équipes de réponse aux incidents informatiques en Afrique ? », *Africa Cybersecurity Magazine*, 2 mars 2020, disponible sur : https://cybersecuritymag.africa.
79. « Que retenir des équipes de réponse aux incidents informatiques en Afrique », Agence nationale de la sécurité des systèmes d'information (ANSSI), 29 septembre 2017, disponible sur : https://anssi.gov.gn.
80. Entretien mené en ligne le 11 février 2025 avec les acteurs sécuritaires et les web activistes au Cameroun, en RCA et au Tchad.
81. *Ibid.*
82. Les entretiens menés à Yaoundé l'ont montré au même titre que ceux menés au Tchad.
83. K. Acakpo, « Cyberattaque contre la BGFIBank : la liste des fichiers volés désormais en accès sur internet », *op. cit.*

Le long chemin de la sensibilisation des usagers

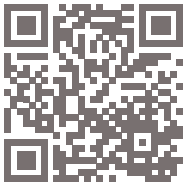
Le manque de connaissances des usagers est apparu sous plusieurs formes au cours de cette recherche. D'une part, durant les entretiens, beaucoup d'enquêtés se sont étonnés de l'existence d'un cadre normatif dans leur pays pour lutter contre la cybercriminalité. D'autre part, le public ne connaît pas les procédures et les modalités de saisine des institutions spécialisées. Par exemple, les citoyens ne savent pas toujours comment procéder pour aller du dépôt de la plainte à la réquisition afin d'avoir des éléments sur l'acte cybercriminel dont ils auraient été victimes. Enfin, beaucoup d'usagers d'internet n'ont pas intériorisé les réflexes de prudence et les pratiques essentielles d'hygiène informatique[84]. Compte tenu de la relative nouveauté de cette technologie, son appropriation est encore parfois balbutiante. Ainsi, une de nos interviewées n'arrivait pas à faire le lien entre le piratage dont elle avait été victime et les faux liens sur lesquels elle avait cliqué avant. Elle ne comprenait pas comment son compte WhatsApp avait été piraté[85].

L'éducation du public aux bonnes pratiques d'hygiène informatique est un chantier en développement en Afrique centrale. Au Cameroun, cette tâche est confiée à l'Agence nationale des technologies de l'information et de la communication[86]. Des campagnes[87] de sensibilisation générales et spécifiques à certains groupes professionnels[88] se multiplient à l'instar du Forum de Brazza sur la cybersécurité et du Forum national annuel sur le même sujet au Cameroun[89]. La sensibilisation du secteur privé aux cybermenaces progresse indéniablement : 67 % des entreprises camerounaises disposent d'une politique de cybersécurité et 46 % d'entre elles effectuent un audit de cybersécurité annuel[90].

84. A. Ducass, « La transition numérique de l'Afrique et les emplois induits. Le risque d'une génération Ninja ? », *Annales des Mines - Réalités industrielles*, 2019/3, 2019, p. 57-62.
85. Entretien mené en RCA le 13 décembre 2024 avec une utilisatrice.
86. « Un atelier d'IA pour donner aux régulateurs du secteur public les moyens d'innover, prédire et mieux servir les citoyens », ANTIC, disponible sur : www.antic.cm.
87. D.-C. Dzonteu, « Gabon : l'Aninf en campagne de sensibilisation contre la cybercriminalité », *GabonReview*, 22 janvier 2020, disponible sur : www.gabonreview.com.
88. L. Ntoutoume, « Cyber assurance : une solution contre la cybercriminalité », *GabonReview*, 8 mai 2018, disponible sur : www.gabonreview.com.
89. Ce forum réunissait les pouvoirs publics et les entreprises afin de procéder à « l'évaluation des éventuelles menaces auxquelles sont exposés les systèmes, à la pose des bases pratiques d'une gouvernance numérique sécurisée pour les pouvoirs publics, à la sensibilisation des jeunes étudiants à la culture de la cybersécurité et aux techniques de protection des données et de détection des menaces cyber ». Voir le « Rapport d'activité – Forum Brazza Cybersecurity – Édition 2021 », SKYTECH CONGO, octobre 2021, disponible sur : https://cybersecuritymag.africa. Sur la dernière édition du Forum national sur la cybersécurité au Cameroun, voir A. Ougock, « Cameroun : Cybersécurité, un engagement national pour la protection des données personnelles », Koaci, 13 décembre 2024, disponible sur : www.koaci.com.
90. «2020 – États de la sécurité des applications en entreprises », Gefona Digital Foundation, 13 mai 2026.

Conclusion

Le développement de la cybercriminalité en Afrique centrale reflète une inégalité inévitable entre les pratiques déviantes du numérique et la capacité des pouvoirs publics à prévenir et répondre à ces menaces. Pour faire face à cette cybercriminalité dont les manifestations vont de la petite escroquerie en ligne au vol de données des banques ou organismes publics, les États d'Afrique centrale ont mis en place des cadres juridiques et des agences publiques spécialisées. Il importe maintenant qu'ils investissent dans les capacités techniques et humaines, la coopération internationale ainsi que dans l'éducation de la population aux bonnes pratiques d'hygiène informatique pour bâtir une politique de cybersécurité plus efficace.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org