REPORT

DIGITAL DECEPTION

Online job scams amid cybercrime vulnerability in Cameroon and Chad

Ado Adamou Abba Ari

INSTITUTE FOR SECURITY STUDIES

CENTRAL AFRICA OBSERVATORY ON ORGANIZED CRIME AND VIOLENCE

AUGUST 2026

Cover: *© Adrienne Surprenant/Bloomberg via Getty Images*

About the ISS
The Institute for Security Studies (ISS) partners to build knowledge and skills that secure Africa's future. The ISS is an African non-profit with offices in South Africa, Kenya, Ethiopia and Senegal. Using its networks and influence, the ISS provides timely and credible policy research, practical training and technical assistance to governments and civil society.

www.issafrica.org

CONTENTS

Acronyms and abbreviations

AI	Artificial intelligence
ANSICE	National Agency for Computer Security and eCertification
ANTIC	National Agency for Information and Communication Technologies
CERT	Computer emergency response team
ECCAS	Economic Community of Central African States
EU	European Union
FCFA	CFA franc (Franc de la Communauté Financière Africaine)
UNODC	United Nations Office on Drugs and Crime

Executive summary

This report provides an analysis of cyber-facilitated fraudulent employment and socio-economic integration scams within Central Africa using a focused comparative case study of Cameroon and Chad. The investigation reveals an adaptive and increasingly transnational criminal ecosystem that takes advantage of the aspirations of the region's digitally connected yet socio-economically vulnerable youth population. Criminals exploit social media and messaging platforms – primarily WhatsApp and Facebook – to carry out social engineering schemes. These scams, predominantly based on advance-fee fraud models, result in financial losses for victims and involve the harvesting of personal data. Some cases lead to recruitment into human trafficking networks, resulting in forced labour and sexual exploitation in the Gulf states and beyond.

The research identifies a link between this form of cybercrime and the broader context of regional instability. The analysis shows how conflicts, such as the Anglophone Crisis in Cameroon and the Boko Haram insurgency in the Lake Chad Basin, create conditions in which these scams can develop by contributing to displacement, economic pressure and weakened institutions. It also indicates that proceeds from these activities may contribute to further instability and reinforce patterns of violence and exploitation in the region. In addition, fraudulent offers can encourage irregular migration towards Europe and the Gulf states, linking digital deception with physical human trafficking.

Current national and regional responses are inadequate and have been outmatched. Legal frameworks are outdated and poorly enforced, and the institutional capacity within law enforcement and the judiciary is limited by a lack of technical resources and specialized training, as well as insufficient cross-border cooperation mechanisms. Policies and strategies fail to translate into practice.

The report analyzes how these online scams operate, the actors and networks involved and the tools and platforms they use. It assesses their scale and impact on victims as well as the effectiveness of current responses. The analysis also identifies key gaps in legal, institutional and operational capacity. The report is structured into six sections, covering the modus operandi of scams; the actors, networks and tools involved; victim profiles and impacts; links to conflict and migration; and weaknesses in prevention systems and national, regional and international responses, before concluding with recommendations.

Methodology

The research focuses on Cameroon and Chad as comparative case studies. While both countries face similar socio-economic and political pressures, they differ in digital infrastructure and connectivity, enabling comparison of how these factors shape scam dynamics. The analysis focuses on scams linked to employment and socio-economic integration, while also considering broader implications for Central Africa.

The research draws on desk-based sources, including reports and data from national institutions, such as the National Agency for Information and Communication Technologies (ANTIC) in Cameroon and the National Agency for Computer Security and eCertification (ANSICE) in Chad, as well as international organizations, including the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (INTERPOL) and the International Telecommunication Union. These are complemented by semi-structured interviews with public officials, representatives of non-governmental organizations and, where feasible, victims of scams. In addition, digital ethnography is used to monitor social media platforms and online forums, including Facebook and WhatsApp, to analyze scam messages, fake online profiles and the structure of virtual networks. These detailed case studies of Cameroon and Chad provide comparative insights into patterns of fraud and institutional responses.

The data was analyzed using thematic analysis, combining qualitative coding of interviews and desk research to identify recurring themes, patterns and trends related to scam methods, actor profiles and systemic vulnerabilities. Quantitative data from surveys and reports was used to triangulate these findings and estimate the scale and financial impact of the scams. The comparative case study approach draws contrasts and parallels between the Cameroonian and Chadian contexts, ensuring that the findings reflect local realities.

While measures were taken to ensure broad representation, the sample of 80 respondents is not sufficient to draw definitive conclusions about online job scams in Cameroon and Chad. The study faces several additional limitations, including limited data resulting from underreporting and security risks, ethical constraints related to victim protection and the clandestine nature of scam operations. It therefore adopts a primarily qualitative approach to ensure data integrity and ethical compliance, with key findings based on informant interviews. In addition, victim testimonies have been anonymized and triangulated with other sources wherever possible.

Key findings

- **Adaptive modus operandi.** Scammers use a multi-stage process (baiting, hooking, playing) tailored to local socio-economic contexts. In Cameroon, this includes impersonation of government initiatives and fake websites. In Chad, with lower internet penetration, fraud is more direct, relying on SMS-based phishing ('smishing') and voice calls ('vishing').
- **Diverse actor ecosystem.** Perpetrators range from opportunistic individuals (e.g. Yahoo Boys[1]) to organized, criminal networks, some with links to transnational syndicates, particularly from Nigeria. This ecosystem is supported by facilitators such as money mules, document forgers and corrupt officials.

- **Human and economic impact.** In 2021, cybercrime caused financial losses of 12.2 billion FCFA (approximately USD$20.2 million) to the Cameroonian economy.[2] Victims suffer severe psychological trauma, social stigma and reputational damage. In some cases, scams are credibly linked to exploitation, including human trafficking.
- **Nexus with conflict and migration.** There is a clear link between cybercrime, conflict and migration. Conflict zones provide a pool of vulnerable individuals, both as victims and recruits. Scams are also used by trafficking networks to move victims under false pretences. In addition, criminal proceeds may contribute to further instability and pose national security threats.
- **Systemic weaknesses in response.** The response remains fragmented and reactive. Key gaps include critically low levels of digital literacy, outdated or absent legal frameworks, under-resourced law enforcement and limited regional cooperation, enabling criminals to operate across borders.

Digital connectivity and access in Africa

Africa's digital landscape has expanded significantly in recent years, with the share of individuals using the internet rising steadily across the continent according to the World Bank.[3] Internet adoption in sub-Saharan Africa remains well below global levels, however, highlighting persistent connectivity gaps despite growth in network availability.

New figures from the International Telecommunication Union show that internet use in Africa has grown at a rate that outpaces the global average, with African connectivity increasing at roughly 16.7% per year since 2005 – more than twice the world's pace – but only about 38% of Africans were online in 2024, compared with roughly 68% globally.[4] This growth reflects considerable progress in network rollout and mobile broadband coverage, yet it also highlights notable gaps: men (43%) are more likely than women (31%) to use the internet; young people aged 15–24 (53%) are more connected than older adults; and urban residents enjoy much higher online access (57%) than their rural counterparts (23%). These trends show that although connectivity is spreading, structural barriers – including affordability, digital skills shortfalls and uneven infrastructure – continue to limit inclusive digital participation across the continent. Internet use in Africa as a whole has increased substantially over the last decade, but the continent still lags behind the global average; only a minority of Africans were online as of the most recent data, even as the absolute number of users continues to climb. This reflects not just the spread of infrastructure, such as mobile broadband and fibre optics, but also ongoing challenges in translating coverage into meaningful usage.

Complementing these macro connectivity figures, Afrobarometer's 2024 data across 39 African countries indicates that digital media use, including regular internet and social media access, has grown significantly but remains unequal across demographic lines.[5] Nearly half of Africans (47%) report getting news from social networks or the internet at least a few times a week, yet this use varies widely by country (from as low as 14% in Madagascar to 82% in Mauritius) and is concentrated among urban, more educated, wealthier, male and younger populations. Despite almost doubling in less than a decade,

these gains in digital media engagement coexist with persistent digital divides that are as large now as they were when overall access was much lower, suggesting that growth alone has not closed underlying barriers to digital inclusion.

While internet connectivity has become essential for innovation globally, Africa still trails most regions: only about 40% of its population uses the internet, compared with roughly 63% worldwide; though this is a significant rise from just 9% in 2012 and 21% in 2017, showing that penetration has quadrupled in the last decade and doubled in the past five years. Southern and northern Africa lead with the highest penetration rates (around 68% and 64%, respectively), whereas central and eastern Africa lag behind at roughly 26% and 25% (see Figure 1).

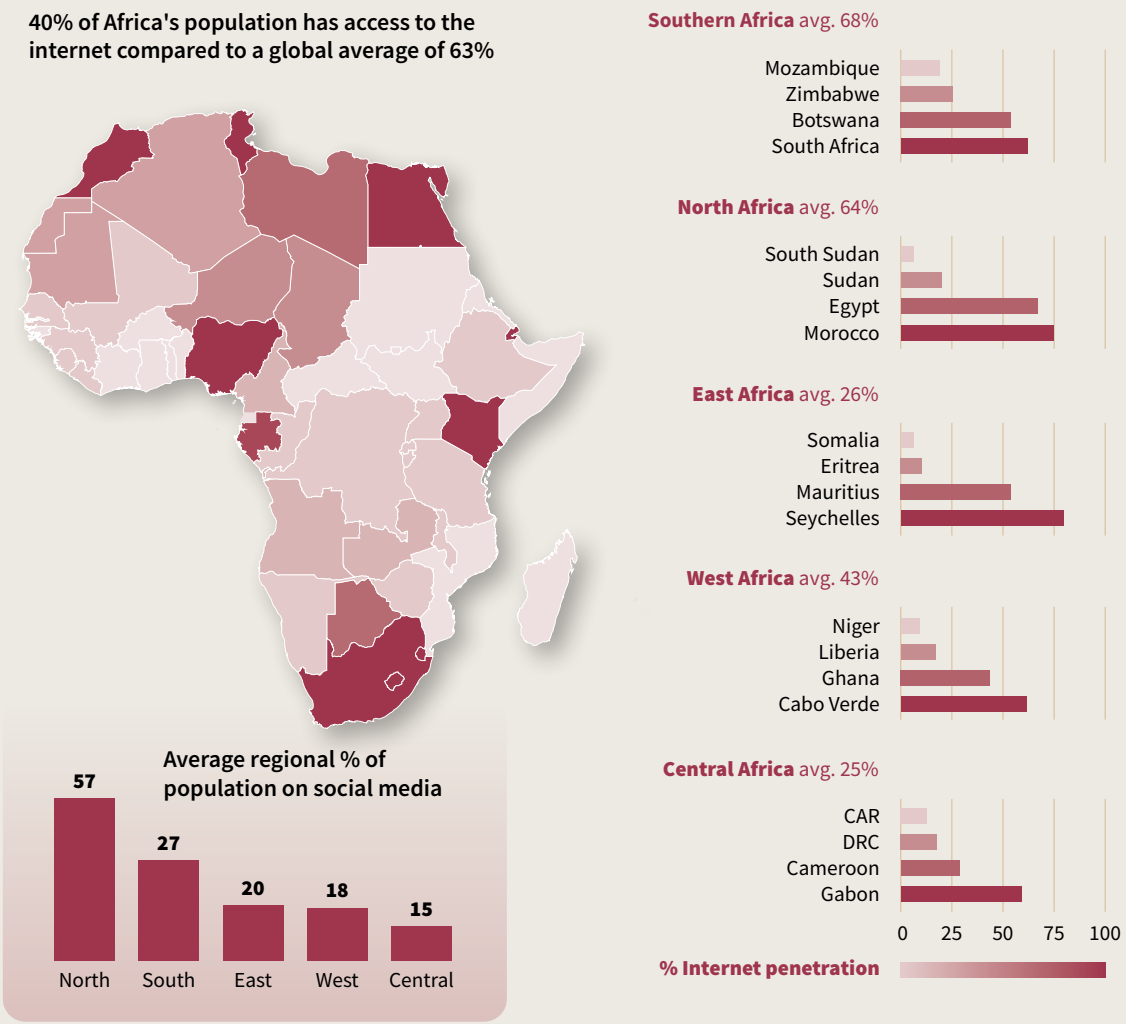

FIGURE 1 Internet penetration in Africa.

SOURCE: Adapted from CRE Venture Capital, Internet penetration, https://www.cre.vc/news-slider/internet-penetration-in-africa-infographic

Key barriers to internet access include affordability of devices and data, low digital literacy and insufficient infrastructure – especially in rural areas. Expanding broadband, mobile networks and data centres will require major investment, which the World Bank estimates at around US$100 billion. Ongoing infrastructure projects – such as the 2Africa subsea cable and Google's Equiano cable, along with major investments from telecom consortia – aim to lower costs and expand access, underpinning projections that Africa's digital economy could reach US$180 billion by 2025 and US$712 billion by 2050 as better connectivity unlocks broader economic and social opportunities.[6]

The rise of digital connectivity and its vulnerabilities in Central Africa

Over the past two decades, digital technology has profoundly transformed life in Central Africa. The proliferation of mobile phones, social media and internet access has become central to communication and commerce. In Cameroon for example, a relatively robust telecommunication sector and the country's strategic location have driven a significant digital boom.[7] A smartphone is often a lifeline and a tool for social mobility for millions of young people in Cameroon.

In Chad, while digital penetration is lower, the shift is no less significant. Mobile phone usage is now widespread, with platforms like Facebook and WhatsApp gaining a firm foothold even in remote communities. This digital integration, although slower, connects Chadians to information and opportunities that were previously out of reach. It is within this context of rapid, yet uneven digital growth that criminal exploitation of this newfound connectivity has taken root.

This digital expansion in Cameroon and Chad reflects broader trends in sub-Saharan Africa, where mobile technology has reshaped connectivity even as structural barriers persist.

In Cameroon, internet and mobile connectivity have grown significantly over the past decade. By late 2025, there were approximately 11 million internet users, representing about 41.9% of the total population. Mobile connections were almost universal, with 29 million cellular subscriptions, equivalent to 96.4% of the population, and 87.5% of these were classified as broadband (3G/4G) capable connections, underscoring widespread access to modern mobile networks.[8] Despite these gains, over 8% of the population remains offline, highlighting persistent gaps between network coverage and actual usage. Reports by the International Telecommunication Union also estimate that up to 75% of the population has access to 3G or 4G services, far ahead of many regional peers in the Economic and Monetary Community of Central Africa (ECCAS).[9] The expansion of smartphones and mobile broadband has broadened access to social media, digital banking and online services, particularly among urban and peri-urban youth.

In contrast, Chad's digital transformation has been slower and more constrained. By late 2025, about 2.79 million people in Chad were internet users, corresponding to a penetration rate of 13.2% of the population – one of the lowest in Africa. Although Chad has seen growth in the number of mobile connections (with mobile penetration rising well above 60% in recent years), the gap between network availability and meaningful internet use remains wide.[10] Limited infrastructure, high costs of access and sporadic or slow broadband services continue to hinder widespread adoption.

Development partners, such as the World Bank, have recently launched broadband expansion and digital skills initiatives aimed at extending access to rural and peri-urban areas and enhancing digital capacities, particularly among youth and women.[11]

Across both countries, the profile of digital citizens tends to skew young, aspirational and urban. In Cameroon, younger age groups – especially those between 18 and 34 – are increasingly represented among internet users, and social media adoption continues to grow. However, digital literacy remains uneven, with many connected citizens lacking the skills needed to navigate digital spaces safely or productively. In Cameroon, the gap between high mobile broadband coverage and relatively lower internet adoption suggests that affordability, literacy and relevance of online services are key bottlenecks. Similarly in Chad, the limited reach of broadband and the high cost of devices and data plans disproportionately affects the young and unemployed, compounding their vulnerability in digital environments.

This growing cohort of young, connected citizens finds itself in a paradoxical position: they aspire to economic opportunity through digital means yet remain exposed to online risks due to employment challenges and insufficient digital skills. These conditions create fertile ground for cybercriminals, who exploit both the increased online presence and the lack of robust digital literacy to carry out elaborate scams and frauds.

The rapid growth of smartphones and mobile broadband is transforming daily life in Cameroon, connecting more people to information and opportunities, and increasing exposure to scams.
© AFP via Getty Images

It is within this context of rapid, yet uneven, digital growth that online job scams have emerged as a particular threat: cybercriminals exploit the conditions created by this digital expansion. Among the many threats posed by cybercrime, online job scams are particularly concerning for several reasons, including:

- **Widespread poverty and unemployment.** Youth unemployment rates, often exceeding 13%, create a context of desperation that criminals exploit. The promise of a job abroad can seem like the only escape, leading individuals to invest their entire savings in fraudulent schemes.
- **Demographic pressure and migration.** With high youth populations, both countries face migration pressures. Many young people see migration as their only path to advancement. Scammers exploit this by offering fake jobs in Europe or other regions, sometimes leading to human trafficking or forced labour.
- **Widespread conflicts.** Ongoing conflicts in the Lake Chad Basin have displaced millions, resulting in a large pool of vulnerable individuals. Fraudulent offers can exploit this desperation, sometimes even serving as a recruitment tool for armed groups or human traffickers.
- **Digital expansion with low literacy rates.** The rapid adoption of social media and messaging apps has outpaced the development of digital literacy. This gap creates a vulnerable user base eager to connect but unprepared for the dangers of misinformation, phishing and fake profiles.

While potentially transformative, the digital boom in Central Africa has also created fertile ground for cybercriminals. They exploit the intersection of widespread connectivity, socio-economic vulnerability and levels of digital literacy to carry out elaborate scams, with online job fraud being a particularly damaging example.

Modus operandi of online job scammers in Cameroon and Chad

Online employment scams in Central Africa rely primarily on deception rather than technical hacking. This section examines the principal methods used by online job scammers in Cameroon and Chad.

Anatomy of an online job scam: A phased approach

A phased approach describes the progression of an online job scam through clearly defined stages, each designed to manipulate the victim. Rather than occurring randomly or opportunistically, these scams operate as structured, multi-stage schemes in which scammers gradually establish credibility, extract financial and personal information and, in some cases, escalate towards physical exploitation. Cyber-facilitated job scams rely on psychological manipulation and social engineering, exploiting trust, urgency, perceived authority and economic vulnerability throughout the process.[12]

The scam typically begins with baiting, in which an offer is crafted to appear highly attractive and often 'too good to be true'. These offers are usually aimed at unemployed individuals or those facing severe economic hardship. To increase their appeal, scammers promise unusually high salaries for low-skilled or unskilled work abroad, require minimal qualifications and advertise generous benefits packages. Perpetrators commonly impersonate or falsely associate themselves with trusted institutions such as government ministries responsible for employment or public services, well-known multinational corporations or reputable international organizations. Forged or promised official documents, including contracts, work permits and administrative authorizations, reinforce the perceived legality and legitimacy of the offer and convince victims that the opportunity is genuine.

Once interest is established, the scam progresses to a contact and trust-building phase. Job offers are widely advertised on high-traffic platforms to enhance their credibility. These often include

social media, where fake profiles and pages on platforms such as Facebook or WhatsApp are used to target specific demographic groups. Scammers also rely on fraudulent websites and emails that mimic professional recruitment agencies, often using cloned or similar email domains. In some cases, fabricated announcements or press releases are broadcast on local radio stations, exploiting the high level of trust such media enjoy, particularly in rural communities.

The next stage involves advance-fee fraud combined with systematic data harvesting. Victims are persuaded to pay a series of small but increasing fees for purposes such as visa processing, administrative formalities or training materials. Payments are typically requested through mobile money services that are difficult to trace. At the same time, under the guise of official recruitment procedures, victims are encouraged to provide sensitive personal information, including identity documents, banking details and other private data. This information may later be used for identity theft or sold on illicit markets.

For the most vulnerable victims, the scam can progress to a more severe phase in which financial fraud gives way to physical exploitation. In such cases, the purported job offer serves as a lure for human trafficking. Victims may be transported to destinations such as the Gulf states, where they are subjected to forced labour or sexual exploitation. Control is often enforced through the confiscation of passports and other identity or travel documents, leaving victims dependent on those who exploit them. At this stage, victims may lose their freedom and remain under the control of their exploiters.

Case of Cameroon: A digitally savvy approach

Cameroon's relatively high level of internet penetration, combined with a large and aspirational youth population, has shaped the country's scam economy. In this context, several forms of online job scams are particularly prevalent.

One common example is the so-called 'Special Youth Emergency Plan' (*Plan d'urgence spécial pour la jeunesse*). In this scheme, scammers fabricate government initiatives presented as official employment or youth support programmes. They rely on counterfeit websites, falsified communications and mobile money payment systems to defraud large numbers of young people.

Another common pattern involves 'Dubai Dream' or 'Canada Job' scams, which target young Cameroonians seeking opportunities abroad. The schemes are typically run through fake recruitment agencies and rely on staged grooming processes, often conducted within WhatsApp groups. Scammers promote false job or migration opportunities and gradually build trust among participants. Communications often contain grammatical errors, language inconsistencies and switches between French and English, which can serve as warning signs. WhatsApp groups help create a sense of community and legitimacy, reinforced by fabricated testimonials from individuals presented as successful beneficiaries.

Case of Chad: Exploiting desperation

Chad's relatively low level of internet connectivity, combined with widespread poverty, has influenced the tactics used by scammers, resulting in methods that are more direct and exploitative. In this context, scams rely less on sophisticated digital platforms and more on widely accessible communication channels targeting economically vulnerable populations.[13]

A predominant strategy involves the use of SMS and voice phishing, commonly known as 'smishing' and 'vishing'. These methods are favoured because they do not require smartphones or expensive internet data, relying instead on basic mobile phones and low-cost text messages and voice calls. Scammers send SMS messages that appear to originate from trusted institutions such as banks, mobile money operators, government agencies or recruitment offices. These messages create a sense of urgency by claiming that an account has been suspended, a payment is pending or immediate verification is required, prompting recipients to reply by SMS or call a provided phone number. This approach is especially effective among users who rely on feature phones or who limit their data usage because of cost.

Vishing complements this approach through direct voice calls or follow-up calls. Scammers exploit the trust associated with spoken communication by impersonating customer service agents, government officials or recruiters. Using persuasive language, they pressure victims to disclose personal information, one-time passwords or mobile money PINs. Voice calls also allow fraudsters to adjust their narrative in real time, address doubts and switch between French, English and local languages to increase credibility. By prioritizing SMS and voice communication over internet-based platforms, these scams eliminate barriers related to connectivity and device access, enabling perpetrators to reach a broader and often more vulnerable population.

Another common tactic involves basic-needs lures that exploit economic insecurity. These scams promote offers framed around immediate survival needs – 'quick money', 'any available job' or 'urgent recruitment' – that target socio-economically vulnerable individuals. Qualifications, documentation and experience are deliberately downplayed to attract those with limited options, particularly refugees and internally displaced persons. Scammers frequently impersonate humanitarian organizations, government bodies or large employers to enhance their credibility. Messages announcing fictitious recruitment opportunities are circulated through SMS, WhatsApp or voice calls, advertising short-term employment with oil companies, cash-for-work programmes, or accelerated recruitment into the military or security services. Victims are then asked to pay processing fees or to provide personal and financial information under the pretext of registration or verification. By aligning fraudulent offers with urgent needs and trusted institutional identities, these schemes reduce scepticism and increase compliance.

A telephone company advertisement in N'Djamena, Chad. Scammers exploit economic insecurity through text messages, phone calls and fake employment offers that prey on urgent needs and limited opportunities. *© Xaume Olleros/Bloomberg via Getty Images*

How online scams differ in Cameroon and Chad

This comparative analysis of cybercriminal practices in Cameroon and Chad is based on interviews with 80 respondents from law enforcement, cybersecurity, financial services, civil society, academia and victims. It reveals a cybercrime landscape dominated by economically motivated offences, with notable national variations (see Figure 2).

In Cameroon, the most frequently reported cybercrime is fraudulent job offers abroad (42%), followed by mobile money fraud (38%) and romance scams (20%), reflecting high youth unemployment and migration aspirations supported by an active diaspora. In Chad, cybercrime is led by mobile money fraud (47%), followed by identity theft (33%) and, to a lesser extent, fraudulent job offers (20%), reflecting the growing adoption of mobile financial services in a largely informal economy.

Across both countries, WhatsApp emerges as the primary attack vector, accounting for approximately 58–60% of cases, largely due to its perceived privacy and credibility. Differences also appear in criminal organization: 82% of respondents in Cameroon report structured links to Nigerian cybercrime networks, compared to a more opportunistic and localized model in Chad, reported by 70% of respondents.

Responses to cybercrime are constrained by systemic challenges, including limited specialized training for investigators (86%) and weak cooperation with technology companies (78%). These constraints are compounded by low levels of public awareness, with 92% of respondents rating societal understanding of cyber risks as 'low' or 'very low'.

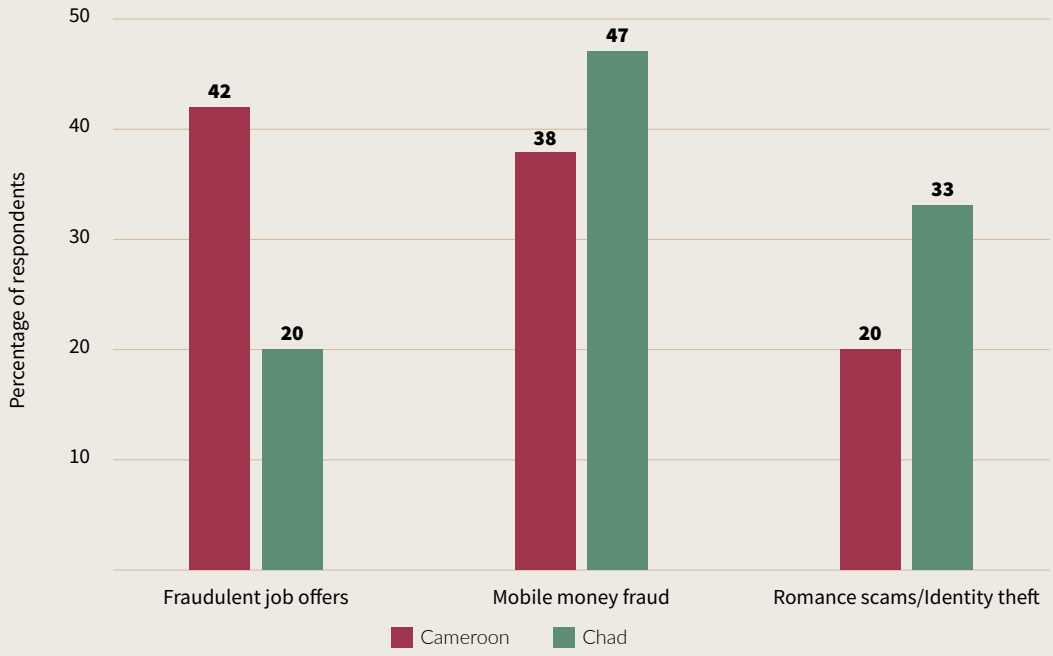

FIGURE 2 Distribution of the three most frequently reported types of cybercrime in Cameroon and Chad.

SOURCE: Data based on key informant interviews, June 2025

Most respondents report a clear shift in cybercriminal practices in both countries, with 94% of participants in Cameroon and 87% in Chad observing significant changes over time (see Figure 3). These shifts include increased professionalism, with fraudulent messages becoming more sophisticated and containing fewer errors, raising suspicions of the use of automated tools or artificial intelligence. Respondents also highlight a move away from mass messaging towards more targeted social engineering, with attackers using social media profiles to personalize their approach. In addition, cybercrime is increasingly carried out through multi-vector attacks, in which initial contact may be made on platforms such as Facebook, continue through private messaging on WhatsApp and end with financial extraction through mobile money services, making detection and intervention more challenging.

In both Cameroon and Chad, social media platforms are the primary channels through which cybercriminals contact victims. Respondents were asked to identify the platform most commonly used to initiate scams (Figure 4).

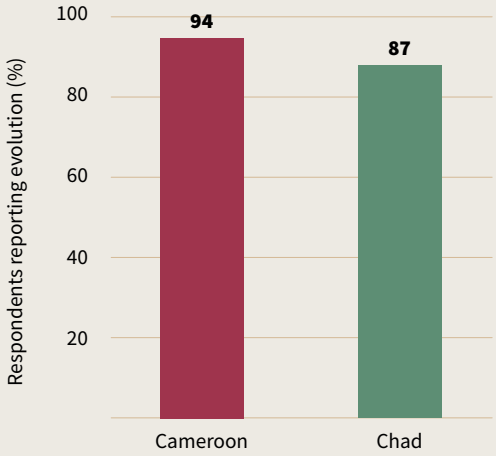

FIGURE 3 Perceptions of how cybercriminal techniques are changing in Cameroon and Chad.

SOURCE: Data based on key informant interviews, June 2025

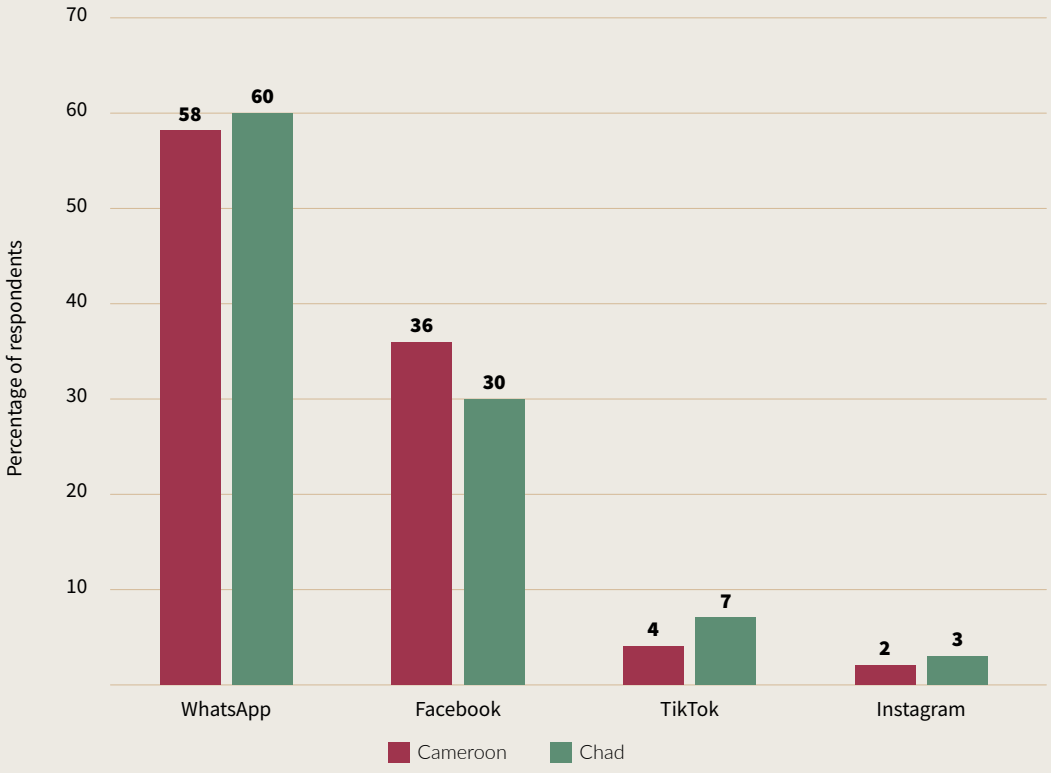

FIGURE 4 Platforms most used by cybercriminals to initiate their attacks in Cameroon and Chad.

SOURCE: Data based on key informant interviews, June 2025

The data shows that WhatsApp is the dominant attack vector in both countries, followed by Facebook, while other platforms such as TikTok and Instagram play a comparatively minor role. This reflects the central role of widely used private communication platforms in facilitating scam activity.

Respondents were also asked whether cybercriminals operate autonomously or in connection with foreign networks. The responses reveal significant differences between the two countries (see Figure 5). In Cameroon, 82% of respondents (particularly law enforcement officers) report links between Nigerian cybercrime networks (such as the Yahoo Boys) and Cameroonian diaspora networks involved in online job and romance scams. In Chad, 70% of respondents describe a more localized and opportunistic form of cybercrime while 30% (particularly experts) point to emerging links with Sudanese or Nigerian networks involved in mobile money fraud. In Cameroon, 82% of respondents report links between local actors and West African transnational cybercrime networks. These findings highlight a more integrated network in Cameroon compared to the 'artisanal' form of cybercrime in landlocked Chad, although the latter may become more professionalized over time.

To assess the challenges faced by the two countries in responding to online job scams, the respondents were asked to identify the main difficulties in detecting and prosecuting cybercriminals.

The obstacles are largely structural and similar in both countries. As shown in Figure 6, 86% of respondents identify a lack of specialized training for investigators and judges as a key challenge. About 78% highlight limited practical cooperation with telecom operators and technology companies (such as Facebook and Google) in obtaining evidence. At least 65% note that regional legal frameworks are outdated or unevenly enforced. Respondents (60%) also point to limited technical resources, including forensic software.

Overall, these findings suggest that responses to cybercrime are constrained more by gaps in technical and legal capacity than by a lack of political will. While a legislative framework exists in Cameroon (notably the 2010 cybersecurity and cybercrime law), enforcement remains weak. These capacity constraints are more pronounced in Chad.

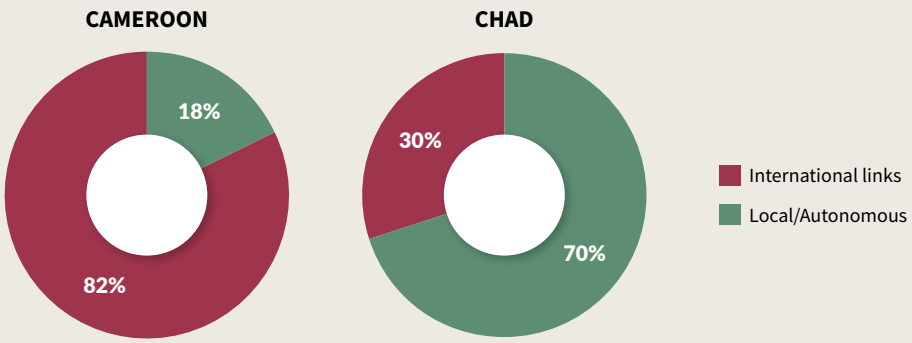

FIGURE 5 Perceptions of cybercriminal organization (local vs international) in Cameroon and Chad.

SOURCE: Data based on key informant interviews, June 2025

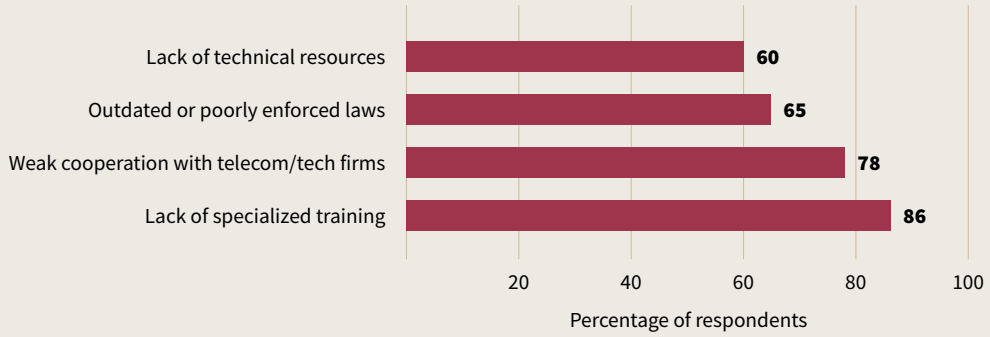

FIGURE 6 Ranking of the main obstacles to fighting cybercrime in Cameroon and Chad.

SOURCE: Data based on key informant interviews, June 2025

The general public are considered highly vulnerable. Across all respondent groups, 92% assess awareness levels as 'very low' or 'low'. A small minority (8%), consisting of experts and academics, rate awareness as 'average', while none consider it 'good'.

A mobile money agent in N'Djamena noted: 'People receive an SMS that says "Your account is blocked, call this number", and they call without a second thought. They give us their codes without understanding the danger.'

While Cameroonian victims lose more per incident (≈132 000 FCFA) than those in Chad (≈58 000 FCFA), the data in Figure 7 also shows a wider range of losses in Cameroon (18 000–738 000 FCFA) compared to Chad (6 000–277 000 FCFA). In Cameroon, losses are typically linked to payments for visas, administrative fees or training, whereas in Chad they are more often associated with mobile money withdrawals and fraudulent humanitarian aid payments. Despite lower losses per incident in Chad, the higher frequency of small-scale mobile money frauds results in significant cumulative economic impact at the national level.

Cybercriminals adapt their strategies to demographic realities. Young adults are the most affected group, while targeting is increasingly balanced across genders (see Figure 8).

The data also indicates that, while the underlying mechanisms of scams remain consistent, their execution is shaped by local conditions. In Cameroon, this is reflected in more complex and transnational operations, whereas in Chad fraud tends to be more direct and opportunistic, targeting economically vulnerable groups.

Country	Average loss (FCFA)	Range (FCFA)	Main type of loss
Cameroon	132 000	18 000–738 000	Payments for visa, administrative fees or training
Chad	58 000	6 000–277 000	Mobile money withdrawals and fake humanitarian aid payments

FIGURE 7 Average estimated financial loss per successful scam in Cameroon and Chad.

SOURCE: Data based on key informant interviews, 2025

Category	Cameroon	Chad	Observations
18–30 years	61%	58%	Youth remain the main target group due to unemployment and digital enthusiasm.
31–50 years	33%	37%	Increasing vulnerability linked to mobile money use and informal employment.
Above 50 years	6%	5%	Minimal exposure, but growing risk of SMS/ voice phishing.
Gender ratio (F/M)	45% / 55%	49% / 51%	Gender gap closing; women increasingly targeted by 'employment abroad' and 'romance' scams.

FIGURE 8 Age and gender distribution of cybercrime victims in Cameroon and Chad.

SOURCE: Data based on key informant interviews, June 2025

Actors, networks and cyber tools

The ecosystem of online fraud in Central Africa – particularly in Cameroon and Chad – is neither random nor isolated. It is a layered, adaptive and increasingly transnational system of actors, networks and digital tools. Understanding this structure is essential for designing interventions and anticipating future trends.

Actors in the cybercrime ecosystem

At the core of the cybercrime ecosystem are individual cybercriminals, commonly young men between 18 and 35 who face limited job prospects but have moderate digital skills. Often called Yahoo Boys, or scammers locally, these actors usually work alone or in small, informal groups. Their activities rely more on social engineering and psychological manipulation than on advanced technical skills.[14] In Cameroon, these individuals are mainly found in urban centres with higher internet access, where they engage in romance scams, fake investment schemes and fraudulent job postings. In Chad, where connectivity is weaker and less reliable, similar actors adapt their methods by relying on SMS messaging and voice calls. In both regions, their main motivation is economic survival, with cybercrime seen as a risky but accessible way to make money.

Beyond these individual actors are organized criminal networks, which represent a more sophisticated and dangerous tier of cybercrime. These groups often operate across borders and are frequently linked to Nigerian confraternities or well-established West African cybercriminal syndicates. Structurally, they resemble corporate organizations, with clearly defined hierarchies that include leaders, coordinators, recruiters and operational 'foot soldiers'. Some networks run informal 'hustle academies', where new recruits are trained in document forgery, scripted social engineering and techniques for evading law enforcement. Their activities extend well beyond online job scams to include romance fraud, sextortion and migration-related schemes. Importantly, these networks often intersect with other illicit economies, such as drug trafficking, smuggling and human trafficking, illustrating a broader convergence between cybercrime and organized transnational crime.

Supporting both individual and organized cybercriminal activity is a broad category of facilitators and enablers. These include recruiters who identify and groom new participants; money mules and informal launderers who move illicit proceeds through mobile money platforms, cryptocurrencies or consumer goods; and technical enablers who create fake websites, clone email domains or provide basic ICT support. In some cases, corrupt officials or complicit intermediaries play a role by turning a blind eye to suspicious activities or by facilitating access to documents and systems. These facilitators blur the boundary between direct perpetrators and logistical support, significantly complicating efforts to dismantle cybercrime networks.

Gender dynamics further shape the cybercrime ecosystem. While men dominate as primary perpetrators, women frequently play strategic roles as recruiters or accomplices, particularly in romance scams, where perceived trust and emotional credibility are critical. At the same time, women are disproportionately represented among victims, especially in scams involving romantic relationships, modelling opportunities or overseas employment. These schemes often expose them to heightened risks of sexual exploitation and trafficking, underscoring the gendered dimensions of cyber-enabled crime.

Network structures and transnational linkages

Cybercrime networks in Cameroon and Chad exhibit a spectrum of organizational forms, ranging from loosely connected peer groups to hierarchical organizations. Many scams originate within small, informal cells where individuals share scripts, templates and tactics through social media or messaging platforms.[15] Over time, successful groups often develop into more hierarchical structures, enabling greater scalability, role specialization and operational resilience.

Transnational linkages play a critical role in this development. The African diaspora functions as a key enabler by providing access to foreign bank accounts, shell companies and cultural knowledge that allow scams to be tailored to victims abroad. Diaspora members may also act as money mules or intermediaries, helping to move funds across jurisdictions. In Cameroon, law enforcement and expert respondents consistently highlight strong connections with Nigerian cybercriminal networks, including confraternities such as Black Axe. Chad, although less digitally integrated, is increasingly exhibiting links to Sudanese and Nigerian groups, particularly in mobile money–related fraud. These connections transform what might otherwise be localized scams into transnational organized crime operations.

Economically, cybercrime thrives in environments characterized by regulatory gaps and weak oversight. Mobile money platforms are frequently exploited for small, rapid and difficult-to-trace transactions, while cryptocurrencies facilitate cross-border laundering in larger operations. Profits are typically distributed hierarchically, ensuring incentives at every level of the organization. In some communities, the circulation of illicit revenues fuels local consumption and informal redistribution, fostering a form of silent complicity that further entrenches cybercrime within the social fabric.

Digital tools and technologies

The effectiveness of cybercrime operations is closely tied to the strategic use of digital tools. Social media and messaging platforms, particularly Facebook and WhatsApp, dominate recruitment and communication, offering direct, private channels that enhance credibility and trust.[16] Telegram and LinkedIn are increasingly used for more targeted or professionalized scams, while Instagram supports the construction of aspirational but false online identities.

Established techniques such as phishing and impersonation remain central. Scammers routinely deploy phishing emails, SMS messages and cloned websites, impersonating banks, government ministries or humanitarian organizations to create a sense of urgency and legitimacy. These methods are especially effective in contexts where institutional trust remains relatively high and digital literacy is limited.

The movement and concealment of funds depend on a combination of payment and anonymity tools. Mobile money services are preferred for small-scale transactions, while cryptocurrencies, VPNs and anonymization techniques are used to obscure identities and launder proceeds in larger or more complex operations.

More recently, the adoption of emerging technologies has marked a significant escalation in sophistication. AI-assisted tools now enable the production of grammatically flawless phishing messages, automated chatbots capable of engaging large numbers of victims simultaneously and, in some cases, voice cloning or deepfake content to reinforce credibility. These innovations substantially increase the scalability, reach and difficulty of detecting online fraud.

Ultimately, the cybercrime ecosystem in Cameroon and Chad encompasses a continuum of actors, from opportunistic individuals to highly organized transnational syndicates, supported by a dense network of facilitators and enablers. Its resilience lies in adaptive organizational structures, diaspora-mediated cross-border linkages and the strategic exploitation of digital tools. Regulatory gaps in mobile money and cryptocurrency systems embed cybercrime within local economies, while emerging technologies such as AI signal a new phase of professionalization. Understanding the interplay between actors, networks and technologies is therefore indispensable for developing effective, context-sensitive counter-strategies in Central Africa.

Victimization, vulnerability and exploitation

Digital scams orchestrated by organized criminal networks in Central Africa inflict significant financial, psychological and physical harm on individuals and communities. Far from being marginal or purely economic offences, online job scams and related frauds represent a serious social and human rights challenge. This section examines the scale of victimization, identifies the populations most at risk and analyzes the continuum of exploitation, arguing that cyber-enabled fraud has become a vehicle for structural violence and abuse.

Scale and economic impact of online fraud

Accurately measuring the scale of online fraud in Central Africa remains difficult due to pervasive underreporting. Many victims do not report their experiences, driven by shame and stigma – particularly in cases involving romance or intimate deception. Underreporting is also linked to a widespread lack of confidence in law enforcement institutions, which are often perceived as ineffective, corrupt or too ill-equipped to respond. In more severe cases, fear of retaliation from organized criminal or trafficking networks further suppresses reporting.[17] As a result, official figures capture only a small fraction of incidents, and the true scale of victimization is almost certainly far greater than available data suggests.

Despite these limitations, existing estimates indicate a substantial economic burden. In Cameroon, the enforcement body ANTIC estimated that cybercrime caused losses of approximately 12.2 billion CFA francs in 2021 alone. In Chad, although comprehensive national figures are lacking, the impact is still severe. Losses are dispersed across thousands of small-scale transactions, particularly through mobile money fraud, reinforcing cycles of poverty and indebtedness. For individual victims, the loss of savings – often accumulated for migration, education or family survival – can constitute an existential crisis, pushing households into long-term financial precarity.

The damage extends beyond direct financial loss. The prevalence of scams erodes trust in digital platforms and institutions, discouraging participation in e-commerce, online services and financial

inclusion initiatives such as mobile money. This erosion of trust poses a systemic risk to digital transformation efforts, effectively acting as a regressive tax on digital participation and undermining the developmental potential of connectivity.

Victim profiles and social consequences

Victimization is not random. Scammers deliberately target populations whose socio-economic circumstances and digital exposure make them particularly vulnerable. Young people and job seekers are prime targets, especially in contexts of high unemployment and limited formal opportunities.[18] Fake job postings and recruitment offers exploit aspirations for upward mobility, both domestically and abroad. Migrants, refugees and internally displaced persons are similarly vulnerable, as they are often seeking pathways out of poverty or conflict, and may lack access to reliable information or protective institutions. Older individuals and those with limited digital literacy are also at heightened risk, as they are less able to identify online deception or recognize warning signs.

The impacts of online fraud are strongly gendered. Women are disproportionately targeted in romance, modelling and caregiving scams, which frequently escalate into sextortion, sexual exploitation or trafficking. These experiences carry significant social stigma, often silencing victims and compounding psychological harm. Men, by contrast, are more commonly targeted through advance-fee job scams, particularly those linked to overseas employment or security-related work.

Beyond economic loss, victims experience lasting psychological trauma. Feelings of shame, depression, anxiety and self-blame are common, often accompanied by a loss of trust in others and in digital systems. Social ostracization and reputational damage further isolate victims, hindering recovery and discouraging engagement with support mechanisms. In this sense, online fraud produces not only individual suffering but also broader social fragmentation.

A pedestrian talks on his phone in Douala, Cameroon. Beyond financial losses, digital scams often leave victims with lasting emotional and social consequences. *Daniel Beloumou Olomo/AFP via Getty Images*

From fraud to exploitation: A continuum of abuse

While financial exploitation is the most visible outcome of online scams, it often represents only the first stage in a broader continuum of abuse. The dominant mechanism is advance-fee fraud, in which victims are induced to make a series of escalating payments for visas, training, administrative processing or fictitious services. Concurrently, many scams involve identity theft, as personal documents and data collected under the guise of 'official procedures' are reused for further criminal activity or sold on illicit markets.

Of greater concern, a growing number of cases show a shift from online fraud to physical and coercive exploitation. Fraudulent job offers increasingly function as recruitment tools for human trafficking. Victims are transported to destinations such as the Gulf states or parts of Asia, where they are subjected to forced labour or sexual exploitation under conditions resembling modern slavery. Control is maintained through document confiscation, debt bondage and threats of violence, leaving victims dependent on their exploiters.

Developments in South East Asia serve as a clear warning for Central Africa. In recent years, tens of thousands of people have been trafficked into so-called 'scam compounds', where they are imprisoned and coerced into conducting online fraud under threat of torture. The mechanisms behind these operations – online recruitment, document seizure, coercion and forced criminal activity – are already present in Central Africa. This parallel emphasizes the risk that the region could become a future hub or supply zone for similar criminal enterprises if current trends are left unchecked.

Finally, online fraud in Central Africa is not merely a cybersecurity issue but a multidimensional threat that reflects and intensifies existing structural inequalities. It generates significant economic losses, inflicts lasting psychological harm and increasingly facilitates human trafficking and exploitation. Addressing this phenomenon therefore requires a holistic response that treats online fraud as a public policy, social protection and human rights challenge, rather than as a narrowly technical problem. Without such an approach, the human cost of digital crime will continue to rise alongside connectivity itself.

Nexus of cybercrime, regional conflict and irregular migration

Online fraud in Central Africa cannot be understood in isolation. Rather, it is an outgrowth of structural factors, most notably protracted armed conflict, economic collapse and irregular migration. Cybercrime, insecurity and irregular migration form a mutually reinforcing triangle. Conflict and instability generate the social and economic conditions that make online scams both attractive and effective; scams, in turn, facilitate human trafficking and irregular migration; and the proceeds of these illicit activities may be reinvested in further violence. Within this cycle, online fraud emerges not merely as a criminal enterprise but as a threat to human security and regional stability.

Conflict and instability as enablers of cybercrime

Armed conflict acts as a force multiplier for cybercrime by dismantling formal economies, weakening state institutions and eroding social trust. In regions affected by violence, livelihoods are destroyed, education is disrupted and young people (often digitally skilled but economically excluded) are pushed towards informal and illicit survival strategies. Cybercrime flourishes in this vacuum, benefiting from limited law enforcement capacity and the normalization of risk-taking behaviours.[19]

The Anglophone Crisis in Cameroon illustrates this dynamic clearly. The protracted conflict in the north- and south-western regions has displaced over half a million people, devastated local economies and reduced employment opportunities for educated youth. Many Anglophones, previously positioned to participate in legitimate digital entrepreneurship, now find themselves excluded from formal labour markets.[20] Within this context of constrained choice, online fraud is reframed by some as a rational economic activity rather than a purely criminal one. Digital skills that might otherwise support innovation and development are redirected into scam operations, embedding cybercrime within a broader narrative of conflict-induced economic collapse.

A similar pattern emerges in the Lake Chad Basin, where the Boko Haram insurgency has produced one of the region's most severe humanitarian crises. Millions of people in northern Cameroon and Chad are internally displaced or dependent on humanitarian assistance. Criminal networks

exploit this vulnerability by impersonating international organizations such as the United Nations High Commissioner for Refugees or well-known NGOs, offering fictitious resettlement programmes, scholarships or overseas employment opportunities. For individuals with no viable prospects and little institutional protection, these fraudulent offers represent a lifeline, making them more willing to pay advance fees or share personal information despite the risks.

Displacement, desperation and cycles of exploitation

Internally displaced persons and refugees occupy a uniquely precarious position within this ecosystem. Displacement fractures social networks, erodes traditional forms of community protection and leaves individuals in a state of severe financial insecurity. At the same time, displaced populations often have a heightened urgency to rebuild their lives, making them particularly susceptible to promises of work, mobility or legal status.

Scams targeting displaced persons frequently mimic humanitarian assistance procedures, demanding 'processing fees' for fake aid programmes, visas or training opportunities. The psychological impact of such deception is profound, compounding existing trauma and reinforcing distrust in institutions. More concerning, the same conditions of desperation that make displaced youth victims of scams also make them potential recruits for cybercriminal networks. In this way, displacement fuels a cyclical relationship in which vulnerability leads to exploitation and exploitation feeds further criminal participation.

People displaced by Boko Haram live in makeshift shelters in Hile Alifa, Cameroon. Displacement can leave vulnerable communities at greater risk of scams and exploitation. *Saabi Jeakespier/ Anadolu via Getty Images*

Cybercrime, irregular migration and human trafficking

Digital scams now function as the primary recruitment mechanism linking cybercrime to irregular migration and human trafficking. Advance-fee fraud is particularly effective because it filters for victims who are already financially committed, compliant and psychologically invested in the promised opportunity. When fraudulent job offers serve as fronts for trafficking operations, the outcome is not irregular migration but modern slavery.

Victims recruited online are transported to destinations such as the Gulf states or major African cities, where passports are confiscated and individuals are forced into domestic servitude, sexual exploitation or coerced labour. The defining elements of human trafficking – deception, coercion and exploitation – are all present, with the digital scam providing the initial deception. In this sense, online fraud is not merely adjacent to trafficking, it is integral to its operational model.[21]

A further dimension of this nexus is the potential diversion of scam revenues into armed conflict. Cyber fraud generates substantial, difficult-to-trace income, especially in regions with weak financial oversight. These funds can be laundered through transnational networks and, in fragile governance contexts, may be used to purchase weapons or finance armed groups. This creates a feedback loop in which conflict enables cybercrime, cybercrime finances instability and instability further entrenches criminal economies.

Taken together, the intersection of cybercrime, conflict and irregular migration in Central Africa forms a complex and growing threat. Armed violence and displacement create desperation; scammers exploit that desperation through digital deception; fraudulent recruitment enables trafficking and forced migration; and the profits from these crimes may support the conflicts that enabled them. Tackling online fraud therefore requires more than technical cybersecurity measures. It necessitates a comprehensive approach that integrates cybercrime prevention into humanitarian policies, migration management and regional security strategies, addressing the underlying vulnerabilities that enable digital exploitation to flourish.

Systemic vulnerabilities and responses to cybercrime

Online employment scams in Cameroon and Chad persist within a set of interconnected structural conditions. These include gaps in digital literacy, limitations in legal and institutional frameworks, constrained law enforcement capacity and uneven regional and international cooperation. Although a range of national, regional and international responses exists, their implementation remains uneven and their effectiveness is limited in practice. The following section examines these vulnerabilities alongside current responses, identifying the key gaps that continue to enable online fraud.

Digital expansion without digital preparedness

One of the most significant weaknesses lies in the rapid expansion of internet access without corresponding investment in digital literacy. Across Cameroon and Chad, millions of new users have entered online spaces with little preparation for the risks that accompany digital participation. This gap is especially pronounced in rural areas and among first-generation internet users, who often interpret online content as inherently credible. Scammers exploit this trust by deploying professional-looking websites, official logos, bureaucratic language and, increasingly, local languages to create a false sense of familiarity and legitimacy.

Economic precarity further amplifies this vulnerability. In contexts marked by high youth unemployment and limited social mobility, offers of jobs, scholarships or migration pathways are not evaluated solely on plausibility but on necessity. Many victims recognize inconsistencies yet proceed because the alternative is continued exclusion. In this sense, scams succeed not because individuals lack intelligence, but because structural deprivation pushes people to privilege hope over caution.

Public awareness initiatives have done little to reverse this trend.[22] Campaigns are often urban-centred, short-term and framed in technical or legalistic language that fails to resonate with those most at risk. Rural populations, displaced persons, women and unemployed youth are frequently excluded, despite being primary targets of fraud. Moreover, coordination among government

ministries, law enforcement agencies, educational institutions and civil society organizations remains weak, and prevention efforts are underfunded. As a result, the most cost-effective line of defence – public education – remains the least developed.

Fragile legal and institutional responses

Institutional and legal frameworks in both Cameroon and Chad are ill-equipped to address cyber-enabled crime.[23] In Cameroon, the 2010 cybersecurity and cybercrime law provides a broad legal foundation, yet enforcement is inconsistent and often criticized for prioritizing state security concerns over victim protection and redress. In Chad, the absence of a dedicated cybercrime statute forces prosecutors to rely on outdated fraud provisions that are poorly adapted to digital offences, resulting in low conviction rates and a climate of impunity.

These legal limitations are compounded by institutional weaknesses. Law enforcement agencies lack specialized training, digital forensic capacity and adequate resources to investigate complex online scams. Even where cybercrime units exist, they tend to be underfunded, isolated and overwhelmed by caseloads. Corruption and bureaucratic inefficiencies further erode public trust, which discourages victims from reporting crimes and reinforces cycles of underreporting.

The transnational nature of cybercrime poses an additional challenge. Scams frequently span multiple jurisdictions, yet law enforcement remains constrained by national borders. Mutual legal assistance processes are slow and cumbersome, while regional cooperation frameworks are underdeveloped or weakly implemented. Criminal networks exploit these jurisdictional gaps, operating across borders with little fear of coordinated pursuit.

Technological gaps and the data deficit

A widening technological gap separates cybercriminals from the institutions tasked with stopping them. Investigators often lack the tools and expertise required to analyze seized devices, trace digital transactions or monitor encrypted communications.[24] Digital evidence is frequently mishandled or rendered inadmissible, undermining prosecutions and reinforcing perceptions of state incapacity.

Equally problematic is the absence of reliable data. Chronic underreporting, combined with the lack of centralized reporting mechanisms or victim support systems, creates a statistical blind spot. Authorities are unable to identify trends, map hotspots or link related cases across regions. Policymakers, in turn, are forced to operate without empirical grounding, while victims remain isolated and unsupported. This data deficit not only weakens enforcement but also obscures the true scale of harm inflicted by online fraud.

Social media platforms and the accountability gap

Global social media and messaging platforms form the primary infrastructure through which scams are conducted. Services such as Facebook, WhatsApp, Instagram and Telegram offer anonymity, scale and speed, while conferring an appearance of legitimacy on fraudulent profiles and advertisements. Although these platforms claim to combat fraud, their moderation systems are largely reactive and poorly adapted to local languages, cultural contexts and regional scam typologies.

Because these companies are headquartered outside the region, local authorities face significant barriers in obtaining user data or timely cooperation. This creates an accountability gap in which platforms benefit economically from user growth while bearing minimal responsibility for the harms experienced by users in Central Africa. The imbalance further entrenches vulnerability, as criminals continue to exploit platform features faster than safeguards are implemented.

Divergent national responses

Efforts to counter online fraud in Cameroon and Chad show that, despite a growing body of laws, agencies and strategies, practical impact remains limited.

Cameroon has developed the most elaborate national response architecture in the Central African sub-region. Its cybersecurity and cybercrime law of 2010 provides a formal legal basis for prosecution, while ANTIC serves as the institutional hub for cyber governance. ANTIC operates a national computer emergency response team (CERT), issues public alerts, provides digital forensic assistance and conducts training programmes for law enforcement officers and judicial actors. These initiatives represent important steps towards institutionalizing cybercrime prevention and response.

Despite this relative advancement, ANTIC's effectiveness remains constrained. Public awareness efforts are largely urban-focused and fail to reach rural or digitally marginalized populations. Institutional rivalries limit information sharing with police and gendarmerie units, while underfunding restricts the agency's ability to invest in advanced investigative tools or sustain public education campaigns. Consequently, while Cameroon's framework is more developed than that of its neighbours, its deterrent effect remains limited and uneven.

Chad presents a more fragile picture. Although a 2015 law created ANSICE, this cybersecurity agency operates with minimal staff and budgetary support and lacks a basic digital forensics laboratory. There is no dedicated cybercrime police unit and investigations are typically conducted by generalist officers with little training in digital evidence, encryption or cross-border data requests. The legal framework itself is broad and insufficiently tailored to contemporary online fraud, resulting in few, if any, successful prosecutions. This institutional vacuum fosters a sense of impunity, emboldening criminal actors.

Regional and sub-regional cooperation: Ambition without execution

Given the cross-border nature of online fraud, regional cooperation is indispensable. Yet, in practice, such cooperation remains weak and uneven. At the continental and sub-regional levels, frameworks such as the African Union's Malabo Convention and initiatives within ECCAS aim to harmonize cybercrime legislation and promote information sharing. However, implementation has been slow and inconsistent, with several states, including Chad, yet to ratify key instruments.[25] Political instability, competing security priorities and limited financial resources have relegated cybercrime to the margins of regional agendas.

In this context, non-state actors, particularly civil society organizations and NGOs, provide victim support, run grassroots awareness campaigns and advocate for policy reform. While useful, these efforts are fragmented and depend on short-term donor funding, which limits their sustainability and scale.

International cooperation and persistent structural constraints

At the international level, Cameroon and Chad face structural constraints that limit their responses to cyber-enabled crime. A central constraint lies in Chad's non-membership in the Budapest Convention on Cybercrime, which is the main multilateral framework for addressing cybercrime through cross-border investigations, harmonized legal standards and mutual legal assistance. Cameroon, by contrast, acceded to the convention in 2022, with its membership officially entering into force in April 2024. This non-membership restricts cooperation with foreign law enforcement, complicates joint investigations and can delay or prevent access to critical digital evidence held abroad. In transnational scams, these gaps create jurisdictional blind spots that can be exploited.

International organizations play an important, though limited, role in addressing these shortcomings. INTERPOL is particularly significant through its coordination of multinational operations, intelligence-sharing mechanisms and secure communication platforms that enable national police forces to exchange information more efficiently. Similarly, institutions such as UNODC and the EU provide technical assistance, capacity-building programmes and specialized training in areas such as digital forensics, cyber investigations and victim protection. These initiatives, however, are often project-based rather than embedded in long-term institutional strategies. As a result, their impact tends to be uneven and difficult to sustain.

These international limitations interact with domestic challenges. Although legal frameworks and specialized institutions exist in both countries, implementation is limited by chronic underfunding, low prioritization of cybercrime and shortages of trained personnel. High turnover within public administrations further undermines capacity, as trained officers are frequently reassigned to unrelated departments or leave public service, leading to a loss of institutional memory. At the same time, organized cybercrime networks benefit from greater financial resources, more advanced technological tools and flexible transnational structures that allow them to adapt quickly.

As a result, state responses are largely reactive. Law enforcement agencies respond to crimes after they occur rather than engaging in proactive prevention or disruption. The mismatch between the scale, speed and sophistication of cybercriminal operations and the limited resources available to national authorities contributes to ongoing vulnerability. Without stronger international legal commitments, sustained investment in institutional capacity and closer integration of global cooperation mechanisms into national strategies, these structural constraints are likely to persist.

Technical and regulatory hurdles in tracing scammer phones

A critical technical barrier to combating online job scams in Cameroon and Chad is the difficulty of tracing the mobile phones used by perpetrators. This challenge stems from a combination of technological improvisation, regulatory gaps and intentional obfuscation by criminal networks, which limits the effectiveness of mobile tracing as a key digital forensic tool.

The main factors contributing to this challenge include:

- **Prevalence of non-registered and prepaid SIM cards.** Most scams are conducted using mobile numbers linked to prepaid SIM cards, which in both countries can be purchased anonymously and in bulk. Despite regulatory efforts to enforce SIM registration, enforcement is inconsistent.

Scammers exploit this by using SIMs registered with fake or stolen identification, creating a dead end for investigators once the number is identified. As a result, tracing hostage takers who call to negotiate and receive ransoms is difficult, as SIM cards are discarded after use. Bandits and hostage takers have used regular telephone calls since the 1990s, particularly in rural and border zones.

- **Use of disposable 'burner' phones and number spoofing.** Sophisticated scammers operate on a 'disposable infrastructure' model. They use low-cost handsets and SIM cards for short periods, often for a single scam campaign, before discarding them ('burner phones'). Furthermore, voice over internet protocol (VoIP) services and caller ID spoofing apps enable scammers to mask their true international numbers with local, legitimate-looking Cameroonian or Chadian numbers, bypassing victim suspicion and misleading initial tracing efforts.
- **Cross-border operations and jurisdictional complexity.** Scam networks are often transnational. A scammer targeting victims in N'Djamena may operate from a border region in Cameroon, using a Cameroonian SIM card, while the command-and-control server is hosted in a third country. Tracing such a call requires real-time cooperation among multiple telecom regulators and law enforcement agencies across borders; this process is hampered by bureaucratic delays, a lack of formal agreements and, often, mutual suspicion. Even within countries, hostage takers negotiating ransoms relocate far from their actual location before calling the victim's relative, directing investigations to that location.
- **Limited technical capacity of law enforcement.** Even when a suspect number is identified, local law enforcement agencies often lack the specialized digital forensics units, equipment and trained personnel needed to investigate cyber-enabled fraud effectively. This includes the capacity to conduct advanced mobile network analysis, retrieve data from seized devices and work with international telecom providers to track more sophisticated tools, such as dual-SIM phones and encrypted messaging applications (e.g. Telegram, WhatsApp) used in later stages of scams.
- **Collaboration deficits with telecom operators.** Effective tracing requires swift, court-mandated cooperation from mobile network operators. In practice, this process can be slow. Mobile network operators may cite privacy laws or require extensive legal paperwork, by which time the scammer has abandoned the number. There is also a lack of automated, real-time data-sharing protocols between mobile network operators and cybercrime units for flagged numbers engaged in fraudulent activities.

Consequently, this tracing difficulty creates a 'shield of impunity' for scammers. It shifts the investigative burden onto victim testimony and digital footprints (e.g. screenshots, bank transactions), which are often insufficient to physically locate perpetrators. It also erodes public trust in the authorities' ability to deliver justice, discourages reporting and perpetuates the cycle of crime.

Conclusions and recommendations

The digital revolution offers significant economic and social prospects for Central Africa, but also creates new criminal risks, including online fraud linked to fake employment and socio-economic schemes in Cameroon and Chad. How perpetrators operate, the effects on victims and the links to regional conflicts and migration are clear. However, national and regional responses show a significant gap between the scale of the threat and the capacity to respond. These findings highlight broader implications for Central Africa and suggest key steps towards building sustainable cyber resilience.

Economic precarity, high unemployment and persistent poverty create fertile ground for both victims and perpetrators. Individuals, often desperate for opportunities, are drawn to promises of rapid wealth or lucrative partnerships, while digitally savvy but economically marginalized youth may view cybercrime as a seemingly accessible path out of poverty.

The expansion of digital infrastructure, coupled with uneven distribution and low digital literacy, amplifies vulnerability. Mobile money, social media and online marketplaces provide both tools for legitimate advancement and opportunities for exploitation. Scammers exploit trust, social networks and emotional vulnerabilities to target individuals and communities.

Several consistent themes emerge:

- Cybercrime in the region has risen due to economic hardship, youth unemployment, widespread digital adoption and weak governance. Online employment and integration scams target vulnerable populations and operate across national borders, increasing their impact.
- These scams have dual consequences: financial loss and psychological trauma for victims, and the erosion of trust in digital platforms, institutions and public processes.

- Legal and institutional frameworks in Cameroon and Chad show uneven progress. Cameroon's cybersecurity and cybercrime law of 2010 and ANTIC have advanced awareness, monitoring and coordination efforts, but underfunding, fragmented coordination and implementation gaps limit effectiveness. Chad's 2015 law establishing ANSICE remains largely inactive, with weak operational capacity, the absence of specialized units and reliance on traditional policing undermining responses to technical crimes.
- Regional frameworks such as the African Union's Malabo Convention and ECCAS initiatives provide a basis for harmonization, but slow ratification and inconsistent implementation limit their effect. Security-focused entities have addressed cybercrime only indirectly, while NGOs and civil society provide fragmented public awareness initiatives and victim support.
- At the international level, engagement with instruments like the Budapest Convention remains partial. Programmes by INTERPOL, UNODC and the EU contribute to training and operations but depend on stronger national ownership for sustainable impact.

Taken together, these findings indicate that, despite progress, persistent challenges – including weak law enforcement, limited judicial capacity, scarce technical resources, poor coordination and socio-economic drivers – make Central Africa's response uneven and largely reactive.

The implications extend beyond Cameroon and Chad. Cybercrime threatens digital transformation, economic development and the credibility of digital services across the region. Scams erode trust in online platforms, discouraging citizens and businesses from engaging in digital economies.

The transnational nature of cybercrime underscores the need for regional coordination. Criminals exploit gaps in national legislation and enforcement, targeting the weakest link in the regional chain. Slow ratification of the Malabo Convention and limited engagement with global instruments exacerbate this vulnerability. Cybercrime also reflects broader governance challenges: weak state capacity, uneven rule of law and resource constraints facilitate not only fraud but a range of illicit activities, undermining state legitimacy.

Socio-economic conditions compound the threat. High youth unemployment and poverty create incentives for engagement in online fraud, normalizing illicit activity. Failure to address these drivers risks creating a 'cybercrime culture' in which fraud becomes a livelihood strategy. The consequences extend globally, as weak enforcement in one region can enable transnational networks, create safe havens and strain international relations. Current national and regional responses to fraudulent online employment scams remain fragmented and critically inadequate. At the national level, Cameroon possesses a relatively advanced legal framework through the 2010 cybersecurity and cybercrime law and a dedicated enforcement body (ANTIC). However, implementation is severely constrained by chronic underfunding, limited technical capacity and weak inter-agency coordination. In contrast, Chad's response remains largely nascent. Their enforcement body, ANSICE, lacks both the financial and human resources required to address cybercrime effectively, while existing legal instruments are outdated and poorly adapted to the collection, preservation and admissibility of digital evidence.

At the regional level, normative instruments such as the African Union's Malabo Convention provide a strong foundation for cooperation, yet ratification and domestication remain slow and uneven across Central Africa. ECCAS, while positioned as a regional coordinating body, lacks concrete operational mechanisms for real-time information sharing and joint investigations, inadvertently creating jurisdictional gaps and safe havens for cybercriminal networks.

Systemically, responses are undermined by low levels of digital literacy among the general population, obsolete legal frameworks, under-resourced and insufficiently trained law enforcement agencies, and the limited accountability of global social media platforms that function as the primary vectors for recruitment and fraud dissemination.

Building resilience against online fraud requires a coordinated, multi-dimensional approach that integrates legal, institutional, technical, socio-economic and cooperative responses. Strengthening legal and institutional frameworks, enhancing technical and operational capacity, improving prevention and public awareness, deepening regional and international cooperation and addressing underlying socio-economic drivers are all essential components of an effective response.

Recommendations

Vulnerabilities in Cameroon and Chad are shaped by the methods employed by cybercriminals and the weaknesses of existing responses. Formal laws and institutions exist but are disconnected from practical effectiveness. Addressing online fraud requires more than policing; it is a systemic challenge linked to governance gaps, limited resources and socio-economic pressures. A coordinated multi-layered strategy is therefore needed – one that strengthens legal frameworks, builds institutional capacity, enhances public awareness, fosters cooperation, continuously monitors conflict-prone areas and addresses the socio-economic factors that shape both victim vulnerability and criminal motivation.

Strengthening legal and institutional frameworks

A coherent legal environment is essential for an effective cybercrime response. Both Cameroon and Chad face challenges due to outdated laws, fragmented mandates and weak enforcement. Harmonization with international standards and adaptation to emerging threats are needed. Cameroon, having ratified the Budapest Convention on Cybercrime, must operationalize its provisions, including streamlined evidence sharing and mutual legal assistance. Chad, lagging in ratification, should accelerate alignment with the Convention. At the continental level, both countries should prioritize practical implementation of the African Union's Malabo Convention to create baseline consistency for cross-border enforcement.

Beyond harmonization, laws must address the technological innovations that criminals exploit. Tools such as cryptocurrencies, AI-driven scams and deepfakes require targeted legal provisions to ensure accountability. Establishing clear standards for digital evidence – including admissibility, preservation and chain of custody – are also essential, as many prosecutions fail due to mishandled or dismissed evidence. Procedural guidelines for judges, prosecutors and investigators can strengthen the judicial process.

Institutional capacity is critical for effective enforcement. Specialized cybercrime units should be established within law enforcement agencies, staffed with trained personnel and provided with dedicated budgets and technical resources. Judges and prosecutors require ongoing training in cybercrime and digital evidence. In Cameroon, ANTIC should expand its rural outreach and strengthen forensic capabilities, while in Chad, ANSICE should be developed into a fully functioning agency, including the establishment of CERTs to monitor threats, coordinate incidents and collaborate regionally and internationally.

Enhancing operational and technical capabilities

Operational and technical capabilities are central to effective cybercrime disruption. Investments in digital forensics laboratories, advanced hardware and software, and personnel training are needed. Governments and international partners should prioritize tools to extract and analyze data from mobile devices, cloud storage and cryptocurrency transactions. AI and machine learning systems can enable proactive threat detection, scanning social media and online marketplaces to identify patterns of fraudulent activity before harm occurs.

A centralized cybercrime intelligence database is also essential. By compiling reports from victims, financial institutions and telecom providers, authorities can identify trends, link cases and track digital footprints. Such intelligence enhances investigative efficiency and supports prosecutions. Interoperability across national and regional systems is critical to enable timely information sharing and coordinated responses.

Prevention and public awareness

Effective responses require proactive public education. Nationwide public awareness campaigns should be multi-platform, combining radio, television and social media to reach diverse audiences. Messaging should be clear and actionable, highlighting common red flags such as advance fees, promises that seem 'too good to be true' and emotional manipulation tactics.

Digital literacy and cybersecurity education should be integrated into school curricula and adult learning programmes, equipping the population with skills to navigate the digital landscape safely. Tailored programmes for vulnerable groups, including the elderly and rural communities, are essential. Accessible victim support services, including hotlines and online portals, should provide guidance, legal assistance and psychological support, recognizing the impacts of online fraud.[26]

Fostering regional and international cooperation

Online fraud transcends borders, requiring coordinated responses. Regional bodies such as ECCAS should formalize platforms for real-time information sharing and joint investigations, with designated cyber liaison officers in each member state. Regular joint training exercises and operational planning meetings can harmonize procedures and support coordinated cross-border interventions.

At the international level, deeper engagement with INTERPOL, UNODC and EU technical assistance programmes is essential. Countries should leverage these partnerships to build sustainable institutional capacity, acquire forensic equipment, establish CERTs and implement effective awareness campaigns. Technical assistance should focus on knowledge transfer, ensuring local ownership and long-term resilience.

Addressing socio-economic drivers

Cybercrime is driven not only by institutional gaps but also by structural socio-economic conditions, particularly high youth unemployment, poverty and social exclusion. Combating cybercrime sustainably requires economic interventions that provide legitimate pathways for income and entrepreneurship. Governments should stimulate inclusive growth, support small and medium enterprises and create opportunities in high-employment sectors such as agriculture and digital services.

Vocational and digital skills training in coding, graphic design, data analysis and digital marketing can equip youth with marketable skills. Programmes should target at-risk individuals and former cybercriminals, offering alternatives to illicit activity. Community-level initiatives, particularly in areas affected by conflict and economic hardship, should combine microgrants, mentorship, psychosocial support and educational programmes to provide pathways out of criminal exploitation.

The fight against online fraud in Cameroon and Chad demands a shift from reactive, narrow law enforcement strategies to a proactive, holistic and coordinated approach. Legal reform, institutional capacity-building, technical innovation, public education, regional and international cooperation and socio-economic development must work in concert. Cybercrime is not merely a policing issue; it is a systemic governance and development challenge. Only a sustained, multi-pronged and collaborative strategy can dismantle the ecosystem of online fraud, empower citizens and create inclusive digital economies that reduce vulnerability. Implementing these recommendations provides an opportunity not just to combat cybercrime but to strengthen institutions, foster social cohesion and secure a more prosperous digital future for all citizens.

Notes

1 'Yahoo boys' is a colloquial term primarily used in Nigeria to describe young individuals engaged in online fraud, including phishing, romance scams and advancefee fraud. The name originates from the early use of Yahoo! Messenger as a tool for soliciting victims.

2 National Agency for Information and Communication Technologies, cited in Pouvoirs d'Afrique, *La cybercriminalité fait perdre des milliards de FCFA au Cameroun*, 8 March 2022; and ITWeb Africa, Cameroon loses 12.2-bn CFA to cybercrime in 2021, 18 October 2022.

3 See: https://data.worldbank.org/indicator/IT.NET.USER.ZS.

4 International Telecommunication Union, Statistics: Global and Regional ICT Data, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Figures for 2024 and annual growth rates since 2005 calculated from ITU's Measuring Digital Development: Facts and Figures 2024.

5 Ecofin Agency, Africa's internet growth outpaces world, but gaps in access remain deep, 5 June 2025, https://www.ecofinagency.com/news-digital/0506-47164-africa-s-internet-growth-outpaces-world-but-gaps-in-access-remain-deep.

6 See CRC, Internet penetration in Africa, https://www.cre.vc/news-slider/internet-penetration-in-africa-infographic.

7 Cameroon Telecommunications Regulatory Agency, 2024 Annual Observatory of the Electronic Communications Market in Cameroon.

8 Simon Kemp, Digital 2026: Cameroon, DataReportal, 8 November 2025, https://datareportal.com/reports/digital-2026-cameroon.

9 ITU, Measuring digital development: Facts and Figures 2025, Available at https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

10 Simon Kemp, Digital 2026: Chad, DataReportal, 8 November 2025, https://datareportal.com/reports/digital-2026-chad.

11 World Bank, World Bank increases access to broadband connectivity in Chad, 25 September 2024, https://www.worldbank.org/en/news/press-release/2024/09/25/world-bank-increases-access-to-broadband-connectivity-in-chad.

12 Eyong Effi Atem, Assessing the gaps in cybersecurity resilience in Cameroon: Challenges and opportunities for strengthening national cybersecurity frameworks, *Journal of Computer and Communications*, 13, 2 (2025).

13 Alima Nzeket Njoya et al, Mobile money phishing cybercrimes: Vulnerabilities, taxonomies, and characterization from an investigation in Cameroon, Towards new e-Infrastructure and e-Services for Developing Countries, 14th EAI International Conference, AFRICOMM 2022, Zanzibar, Tanzania, December 2022, https://eudl.eu/proceedings/AFRICOMM/2022.

14 Emmanuel Niyikora, Cybersecurity risk assessment methods for digital financial services in Sub-Saharan Africa, doctoral dissertation, Walden University, 2025, https://scholarworks.waldenu.edu/dissertations/18000/.

15 Yushawu Abubakari, The reasons, impacts, and limitations of cybercrime policies in Anglophone West Africa: A review, *Przestrzeń Społeczna*, (2021).

16 Victor A Adewopo et al, Comprehensive analytical review of cybercrime and cyber policy in West Africa, *Journal of Electrical Systems and Information Technology*, 12, 1 (2025).

17 Newman U Richards and Felix Eboibi, African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?, *International Review of Law, Computers & Technology,* 35, 2 (2021).

18 O T Adisa, The impact of cybercrime and cybersecurity on Nigeria's national security, 2023.

19 Shai Farber, The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications, *Security Journal,* 38, 1 (2025).

20 Fonjock Harris Kunju, Digital warfare: Exploring Cyber criminality amidst armed conflict in the Southwest region of Cameroon, *Journal of Research in Social Science and Humanities*, 3, 10 (2024).

21 Alex Motshwanetsi Mathole, Coverage of modern slavery and human trafficking in national risk assessments within Sub-Saharan Africa, United Nations University Centre for Policy Research, March 2023, https://collections.unu.edu/eserv/UNU:9093/National_Risk_Assessments_vFINAL.pdf; Oluwole Ojewale, Shadow of death: the criminal economy of banditry and kidnapping in northwest Nigeria, *Security Journal*, 37, 4 (2024); Freedom C Onuoha, The terrorism-organized crime nexus in the Boko Haram insurgency in Nigeria, in *The Nexus Between Organized Crime and Terrorism.* Cheltenham: Edward Elgar, 2022.

22 Alain Hugues Obame, *L'usage d'Internet comme circonstance aggravante de responsabilité pénale, une introduction*, *ADILAAKU – Droit, politique et société en Afrique*, 2, 1 (2022); Tim Hall and Ulrike Ziemer, Cybercrime in Commonwealth West Africa and the regional cyber-criminogenic framework, *The Commonwealth Cybercrime Journal*, 1, 1 (2023).

23 GN Gasu, Legal responses to combat the menace of cybercrime in sub-saharan africa: A comparative analysis, *GLR*, 4 (2022).

24 Maria Grazia Porcedda and David S Wall, Modelling the cybercrime cascade effect in data crime, in IEEE European Symposium on Security and Privacy Workshops, 2021.

25 Ugah John Otozi et al, Cybercrime and its negative effects in developing countries, *Journal of Mobile Computing and Application*, 11, 4 (2024).

26 Tim Hall and Ulrike Ziemer, Cybercrime in Commonwealth West Africa and the regional cyber-criminogenic framework, *The Commonwealth Cybercrime Journal*, 1, 1 (2023).

ISS | INSTITUTE FOR SECURITY STUDIES

The Institute for Security Studies (ISS) partners to build knowledge and skills that secure Africa's future. The ISS is an African non-profit with offices in South Africa, Kenya, Ethiopia and Senegal. Using its networks and influence, the ISS provides timely and credible policy research, practical training and technical assistance to governments and civil society.

issafrica.org

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

The Global Initiative Against Transnational Organized Crime is a global network with 800 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

globalinitiative.net