European Journal on Criminal Policy and Research (2024) 30:359–378
https://doi.org/10.1007/s10610-024-09597-7

ORIGINAL RESEARCH

How do Ivorian Cyberfraudsters Manage Their Criminal Proceeds?

Cristina Cretu-Adatte[1] · Renaud Zbinden[1] · Luca Brunoni[1] · Hazel Bunning[1] · Josselin Wilfred Azi[2] · Olivier Beaudet-Labrecque[1]

Accepted: 19 July 2024 / Published online: 31 August 2024

Abstract
This article delves into the intricacies of managing illicit financial gains among Ivorian cyberfraudsters, shedding light on the findings of a field study conducted in Côte d'Ivoire by Swiss and Ivorian research teams. The study involved interviews with cybercriminals, law enforcement officials, and subject matter experts, in order to answer a specific question: What strategies do Ivorian cyberfraudsters use to manage and launder the criminal proceeds originating from romance scams and sextortion? The results explore the tactics employed by cyberfraudsters to obfuscate the illicit financial flows, their organizational structures, and the strategies they employ in managing and using their gains. It confirms certain elements from the scientific literature, in addition to introducing new insights for a better understanding of the processes of money laundering and the use of illicit funds. The article also unravels the multifaceted challenges encountered within the anti-money laundering framework in the context of cybercrime and raises avenues for further reflection and future work to enhance the fight against this scourge.

Keywords Cyberfrauds · Money laundering · Management of cybercriminal proceeds · Côte d'Ivoire · Romance scams

Introduction

A substantial and probably predominant share of crime has shifted to the online sphere, presenting opportunities for motivated fraudsters, but also challenges for law enforcement in adapting to the evolving cyber threats (Interpol, 2022; Federal Bureau of Investigation, 2021). Not only do cyberfrauds have heavy financial and psychological consequences (Bailey et al., 2021; Cross, 2023), they also hinder the global, sustainable, and digital economic development, impact the welfare system, and affect the well-being of populations (ECOWAS, 2021; Interpol, 2021). Despite the absence of indicators to assess the threat and harm from cybercrimes or the costs the incurs, there is consensus on their drastic increase worldwide (FATF et al., 2023; Levi, 2017).

Extended author information available on the last page of the article

West African countries bear some of the costs of cybercrime, especially of cyberfraud, as the swift digitalisation has provided opportunities for young people driven by economic hardships affecting both themselves and their families. These readily accessible avenues for profit adversely affect their judicial system, economic development, stability, and tarnish their image (Atta-Asamoah, 2009; Trend Micro & Interpol, 2017). Moreover, while victims are still targeted abroad, they are increasingly reported within West African nations themselves (Boateng et al., 2011; Gueu, 2013; Wannenburg, 2005). In addition, cybercrime is associated with international e-commerce involving cybercriminal activities and is also linked to a perception of social success among young people (Azi, 2021; Akadjé, 2017).

Cyberfraudsters, demonstrate a propensity to coordinate their activities into networks with fellow individuals from various sectors, including other fraudsters, law enforcement officials or financial intermediaries, to maximise efficiency and earnings (Ahissan et al., 2017; Azi, 2021). In early studies, it was already recognised that these networks employ members operating on a transnational scale (Addo, 2006). Recent international reports highlight a new category of cybercriminals characterised by higher organisation levels and professionalism (Aman, 2023; FATF et al., 2023; Trend Micro & Interpol, 2017). Their activities focus on profit and money laundering with more sophisticated techniques than those of less experienced fraudsters. These cybercriminals seem to channel money through international social connections and employ multiple strategies to minimise traceability of the criminal proceeds.

Côte d'Ivoire is considered to be "one of the hubs for cybercriminals and [listed] among high-risk areas for electronic transactions in Africa" (Akadje, 2011). Despite the absence of sub-regional statistics, the political interest and pressure demonstrated by the establishment of legislative and operational frameworks to combat cybercrime in 2011 and money laundering in 2016, in Côte d'Ivoire, supports Akadje's (2011) assertion, and illustrates the seriousness of the threat. In Autumn 2022, the the Institute of economic crime investigation (ILCE), based in Neuchâtel, Switzerland and the Criminology Training and Research Unit of the Félix Houphouët Boigny University, based in Abidjan, Côte d'Ivoire conducted a study aiming to examine the resources and methods used by Ivorian cyberfraudsters for their activities, as well as the illegal financial transactions and money laundering associated with them. The study enhanced our understanding regarding the similarities between the *modus operandi* of Ivorian romance scammers and video blackmailers, but also the mechanisms used to circumvent the law and to get to their criminal proceeds without much risk. The present paper is an initial endeavor to explore the findings obtained through interviews with Ivorian cybercriminals, also known as "brouteurs", concerning their management of criminal proceeds derived from the most commonly perpetrated online scams in Côte d'Ivoire, namely romance scams and sextortion.

As a reminder, the *modus operandi* employed by the *brouteurs is* characterised by the creation of fake accounts on social networks or dating websites, using falsified or stolen identities (Barnor et al., 2020; Fortin, 2013; Sorell & Whitty, 2019; Tasso & Ouassa Kouaro, 2014; Wang & Topalli, 2022). The initial objective in a romance scam is to establish a trust relationship with their clients (victims), subsequently orchestrating a dramatic event that they exploit to manipulate and persuade victims into sending money (ibid.). Sextortion, with initial stages similar to those of the romance scam, involves convincing the victim to undress, take intimate photos or videos, and then extorting money by blackmailing the victim (O'Malley & Holt, 2022). These two types of cyberfrauds can operate in parallel,

motivated by financial gain, but at a different pace. The relationship is either quickly established, often with male victims, or takes longer to develop but yields more profit, particularly with female victims (Cross et al., 2022). Given the similarity in the execution of such scams, as well as the organisation of *brouteurs* within common networks, it is likely that the methods of managing and consequently laundering criminal proceeds are shared different fraudsters. This paper will commence by providing a review of the Ivorian context of the anti-money laundering regime and a literature review to delve into the money laundering of cybercriminal proceeds research methods and results. That will be followed by an outline of the objectives addressing the issue of managing illicit assets and the mechanisms employed by cybercriminals to circumvent the law. The methodology and findings will elucidate the interviews conducted with cyberfraudsters and stakeholders in cybercrime, as well as money laundering prosecution. Finally, the discussion will offer insights drawn from the study's results regarding the possibilities of managing criminal proceeds by Ivorian cyberfraudsters and the conclusion will provide the limitations of the study and further implications for policy and research.

Ivorian Context

Despite the absence of a consensus regarding the concept of money laundering, Levi and Soudijn (2020) explain essential factors that could influence the strategies chosen by criminals to acquire and launder their proceeds, such as the national anti-money laundering regime, as well as the type of crime, the revenue, and medium to long-term objectives of the offender. In this section, the choice has been made to describe the first essential factor impacting the decision of money laundering mechanisms.

Since the publication of the first Mutual Evaluation Report in 2012, the fight against money laundering in Côte d'Ivoire has made significant progress. The country has moved forward with the adoption of the Anti-Money Laundering Law in 2016, the National Risk Assessment in 2019, the establishment of a specialized prosecutor's office in 2020 (PPEF, Pôle Pénal Economique et Financier), and the development of a national strategy adopted in 2021. These various elements are highlighted in the second Mutual Evaluation Report leaded by the International Monetary Fund in 2022 and adopted by the Inter-governmental Action Group Against Money Laundering in West Africa (GIABA) in 2023. This document notably underscores the importance of cybercrime as a predicate offense to money laundering cases in Côte d'Ivoire, which is expressly claimed to be a priority by the Ivorian Financial Intelligence Unit (CENTIF), by its President, and statutory members.

Between 2017 and 2021, 172 suspicious transaction reports mentioned acts of cybercrime, while 64 reports cited scams out of a total of 2306 reports. It is worth noting that some confusion persists both in the National Risk Assessment and in the Mutual Evaluation Report regarding the distinction between scams and cybercrime, a confusion exacerbated by a footnote in the second Mutual Evaluation Report mentioning that cases of cybercrime may have been recorded as scams. However, cybercrime is the most frequently mentioned predicate offense in suspicious transaction reports. In fact, 1785 out of 2306 suspicious reports do not specify a specific offense.

Despite the claimed priority and the number of suspicious transactions linked to cybercrime reported, it is worth noting that between 2017 and 2021, no dissemination reports were forwarded to prosecutorial authorities for cybercrime cases, while 77 were forwarded

for scam cases, which is the most common predicate offense mentioned in the dissemination reports. Since its creation in 2020, the PPEF has handled 167 money laundering cases. There are unfortunately no statistics available on the predicate offenses related to the cases.

Finally, and as highlighted in the latest Mutual Evaluation Report, Virtual Assets Service Providers (VASP) are not regulated and therefore not subject to anti-money laundering obligations. This is interesting, especially considering that some VASP offer their services in the country, notably by allowing the exchange of cryptocurrencies from mobile money accounts.

Literature Review

As highlighted by Gueu (2013) in his article describing the growing trend of cyberscams in Côte d'Ivoire around 2012, the culmination of the scamming process often revolves around obtaining money, as individuals seek to address financial difficulties and unemployment faced by their families and communities (Adou, 2022; Konan et al., 2022; N'Guessan, 2014).

(2019 The risk of raising suspicion and getting caught while receiving the criminal income underscores the significance of processes such as recovering and reinvesting illicit money to conceal its origin (Kruisbergen et al. 2019). In this article, these practices are understood as money management, where money, once received, doesn't necessarily have to be laundered to be used, such as for everyday expenses (Horgby et al., 2015).

Mirroring the approach of Kruisbergen et al. (2019), this brief literature review chapter presents two sections: the first focuses on the reception techniques, encompassing the transfer and the withdrawal of illicit funds, while the second focuses on the concealment techniques of the proceeds, encompassing both spending and investment, as well as money laundering strategies.

Reception Techniques

The focus on techniques employed by cybercriminals for the reception of illicit money, particularly in the context of cyberscams originating from West Africa, remains limited in the existing literature. However, understanding these techniques is crucial as cybercriminals seek to obscure money flows or eliminate the traceability of their ill-gotten gains to guarantee a higher level of impunity. Kruisbergen et al. (2019) assert that traditional money laundering methods are favoured not only by groups engaged in conventional criminal activities, but also by organised cybercrime groups. So, basically, the techniques employed by cyberfraudsters, such as the Ivorian networks, could be similar to those used by cyber attackers, for example, as long as they are organised. Similarly, within the context of this article, it is posited that the laundering techniques employed by cyberfraudsters are akin to those used by other categories of cybercriminals.

One prevalent technique observed to obscure the traceability of the illicit proceeds is the use of money mules for fund transfer (Abdul Rani et al., 2023; Bekkers et al., 2023; Custers et al., 2019; Kruisbergen et al., 2019). Money mules are typically recruited through social media, other online platforms or work-at-home job offers and can also be known by cyberfraudsters. They can be promised a certain percentage of the transferred sum, which they may or may not receive depending on the ties they have with the fraudster. It is recognised

that in romance scams cases, victims can be proposed money muling services during the deployment of the script (FATF et al., 2023; Grandjean et al., 2022).

In a prevention message, the Federal Bureau of Investigation (n. d.) categorises money mules based on their level of knowledge of the fraudulent scheme. As such, unwitting or unknowing mules believe in the offer of a job or a relationship without realising its fraudulent nature; witting mules should have realised it's a scheme, while complicit mules are fully aware of their role in opening accounts or transferring obscured money, whether within local or international networks. This categorisation is crucial when legally analysing the liability of third parties whom criminals use to achieve their goals. For example, according to Ivorian law, if a money mule had no reason to suspect that the assets they handled came from an offense, they are not punishable. On the other hand, if the cybercriminal involves accomplices or facilitators who are aware of the criminal activity, the money laundering offense is committed.

Ivorian studies explain that there are accomplices within networks who assist cyberfraudsters in transferring or receiving illicit gains. In exchange for their assistance, these accomplices may receive returns ranging from 10 to 50%, depending on the role and/or complexity of the operation (Adou, 2022; Ahissan et al., 2017; Akadje et al., 2018; Bazare et al., 2017; Gueu, 2013). While these individuals could fall under the category of the complicit mules, it's worth noting that money mules are not commonly addressed in the scope of these studies or measures. These people could also fall under the category of professional money launderers, offering specific money laundering services to the cybercriminals (Levi & Soudijn, 2020). Indeed, the literature suggests that accomplices function more like information operators of financial systems, operating in separate organised groups under a "crime-as-a-service" model (FATF et al., 2023; Lusthaus et al., 2023). Accomplices play a critical role in effectively distancing the cybercriminals from the initial source of funds and relocating the funds, often occupying peripheral roles within criminal networks (Kruisbergen et al., 2019).

Additionally, the adoption of various electronic payment systems, such as Western Union, Paypal, Money Gram, prepaid cards, vouchers, or bank account transfers, enhances complexity of money trails, facilitating rapid cash retrievals (Odinot et al., 2017). The illicit manipulation of the banking system with the aid of accomplices, the establishment of shell corporations or fictional businesses to legitimate sending money, the use of money mules and cash drops, along with wire transfers, appear to be effective means for receiving illicit proceeds, despite the conventional nature of these methods. Simultaneously, McGuire (2018) emphasizes the growing recognition of more sophisticated digitally-driven approaches, such as the adoption of cryptocurrencies. While certain empirical studies reference electronic currencies (Custers et al., 2019; McGuire, 2018; Nazzari, 2023; Paquet-Clouston et al., 2019; Soudijn, 2019), whether they are primarily used for receiving illicit proceeds or laundering them remains somewhat ambiguous. In spite of the rising prominence suggested by experts regarding the potential displacement of traditional techniques, cybercriminals have the tendency to exhibit surprising levels of unsophistication.

Soudijn (2019), through the analysis of crime pattern reports from the Dutch National Strategic Threat Assessment of Organized Crime Report, has highlighted the use of both traditional and novel money laundering techniques by groups involved in fraud or cyber-enabled crimes. Among the innovations observed are the use of prepaid debit cards, virtual currencies, crowdfunding, payment service providers, exploitation of legislative loopholes,

and the hawala system – underground bankers which not only facilitate the transfer of money but also provide means for storing money. Among the techniques demonstrating continuity in their use between 2004 and 2016 are expenditure and investment activities, which are discussed below. This suggests that criminals innovate ways to obscure the origin of money and ensure its untraceability despite legislative developments and the tightening of compliance regulations for financial intermediaries and anti-money laundering regimes.

However, the most effective method of obscuring traces is the use of cash. As such, cash is still preferred, especially among cybercriminals, due to the fact that cash leaves no paper or digital trails, the anonymity provided and the difficulty of finding the origin (Custers et al., 2019; European Police Office, 2015; Kruisbergen et al., 2019; Soudijn, 2019). Using cash enables cybercriminals to bypass concerns about spending money; once withdrawn, they treat it as if it's already laundered, facilitating its reintroduction into the local economy.

Concealment Techniques

A slightly larger share of researchers focused on the spending and the concealing of criminal proceeds once the cyber offender pocketed his loot. Akadje et al. (2018) described, in their study on Ivorian cyberscammers, three distinct modes of using illicit criminal proceeds. These include expenditures in material and financial support, leisure activities, and for investment purposes. Koné (2015) observed Ivorian young fraudsters with flashy four-wheel-drive vehicles, stacks of banknotes, champagne bottles, and ostentatious lifestyles, often funding an extravagant entourage, express lavish displays of wealth. Direct spending within online shopping platforms, the exchange of funds into bitcoins, and investments in businesses such as transfer agencies, cybercafés, the resale of computer equipment, and transportation, represent the transformation of ill-gotten gains into symbolic capital emphasising the reputation of cyberfraudsters (Akadje et al., 2018). Consequently, these actions generate new jobs and integrate cybercriminal proceeds into society, thereby legitimising cybercrime in the eyes of the public and emphasizing the good will of the perpetrators.

Through interviews with active and incarcerated cybercriminals, McGuire (2018) obtained similar results: 15% of cybercriminals spend their money on daily expenses, 20% spend their money on hedonistic activities, and 15% use cybercriminal proceeds to impress their peers. Moreover, 30% of the cybercriminals invest their revenues into assets such as property, and 20% of them reinvest in further criminal activities.

Kruisbergen et al. (2019) describe findings that reveal a range of techniques employed for concealing and money laundering. These tactics include document forgery, cross-border transfers, as well as IT-driven methods such as cryptocurrencies and prepaid cards and activities such as gambling at casinos, the purchase of electronic currencies and vouchers, the procurement and resale of goods, or the establishment of complex networks of shell companies (Custers et al., 2019; Odinot et al., 2017).

Returning to Soudijn (2019) and the tactics still employed by criminal groups for money laundering, the "golden oldies" include loanbacks and fictitious turnover of legitimate cash-intensive businesses, investment in real estate, fictitious gambling profits, and trade-based money laundering. The author suggests that it is important to consider the continuity of these techniques, which in the majority of cases, do not involve technology. Therefore, it would be beneficial to question why detection and enforcement efforts are insufficient to deter the use of these techniques.

Richet (2013) also explained that money laundering involves online channels, enabled by e-currencies, online games, and micro-laundering tactics that leverage small-scale electronic transactions through mobile banking, micro muling jobs, thereby allowing the laundering of small sums incrementally. Nizovtsev et al. (2021) adds to this spectrum of techniques e-auctions and telemarketing.

Collectively, these findings illuminate the multifaceted strategies that represent different techniques used to circumvent the law established to combat cybercrime, and that cybercriminals employ to exploit and launder their illicit gains. The mechanisms for managing criminal proceeds obtained by Ivorian cybercriminals have not been studied yet. Research on this highly relevant and current theme, considering the increasing numbers of cyber victimisations across the world would provide both theoretical and practical insights to enhance the legal framework and societal response to cybercrime.

Objectives

The purpose of this paper is to give a first overview of how Ivorian cybercriminals manage their illicit proceeds. This study aims to provide insights into the methods employed by cybercriminals to circumvent the legislative and operational frameworks. The research question is: what strategies do Ivorian cyberfraudsters use to manage and launder the criminal proceeds originating from Ivorian cyberfrauds?

The specific objectives of the study are to identify the strategies and mechanisms used by Ivorian cybercriminals in managing their illicit gains through semi-structured interviews with cyberfraudsters and institutional actors related to the cybercrime and money laundering prosecution; and, to question the effectiveness of the existing legal framework and undertaken actions in deterring cyberfraudsters from engaging in money laundering activities.

Methods

Research Strategy

The primary data came from semi-structured interviews. This approach was preferred, as it allows for an understanding of the practices and perspectives of the actors in relation to social contexts (Blanchet et al., 1985; Yin, 2011). In this study, conducted in a little-known topic in the perspective of cyberfrauds, the interviews helped target the themes to be discussed and adapt them as the conversations with individuals progressed.

Firstly, various institutions involved in the fight against cybercrime at different levels, including political, judicial, correctional, law enforcement, scientific, banking, were identified through a preliminary study of the Ivorian context. In the absence of available data to analyse the practices of cybercriminal actors and cybercriminal money laundering, interviews were conducted with 18 representatives of these institutions, approached through a key informant. The interviews lasted approximately one hour and took place in comfortable locations for the interviewees, such as their offices or restaurants. The participants discussed topics related to daily practices within the various institutions, collaborations and shared information, obstacles in combating cybercrime, and the need to improve anti-cybercrime

measures. Participants displayed a keen interest in the study, emphasising their willingness to engage and their desire to establish future collaborations.

Secondly, eighteen cyberfraudsters were approached through another key informant. A combined method of non-probabilistic sampling, namely snowball sampling and purposive sampling, was used to meet with ten incarcerated scammers regardless of whether they were active or not, and eight scammers that were not in detention, regardless of whether they were active or not. Meetings with incarcerated scammers were held in the presence of the socio-educational service in a room within the Abidjan Detention and Correction Center (MACA). Meetings with scammers who were not in detention were held in maquis or cafes in Abidjan.

The presence of the key informant at most of the interviews with the participants fostered trust and facilitated the smooth flow of discussions. The key informant translated or rephrased the discussions into *nouchi*, the Ivorian slang. The topics discussed during the exchanges, which sometimes resembled life stories, included the type and number of offenses committed, the amounts demanded or obtained, the resources available for committing offenses, the chosen modus operandi (applications, manipulation techniques, fake profiles used, targets, etc.), the facilitators sought during criminal activity, as well as educational or career prospects.

It was specified at the beginning of the interviews that no information would be used for any purpose other than research and that the goal was to improve the prevention of the phenomenon of *broutage* and the conditions that lead to it. Additionally, in cases of hesitation or non-response to certain questions, the interviewers tried to continue the discussion with minimal disruption. The information was collected by handwritten note-taking on physical paper, and no interviews were recorded on external devices.

Compliance with Ethical Standards Obtaining informed and voluntary consent from each participant was crucial, whether they were institutional or cybercriminal actors. Clearly explaining the study's objectives and the measures taken to preserve their anonymity and data confidentiality was a priority during the interviews to establish trust between the interviewers and interviewees. Consequently, in order to protect the participants' identities, institutional names rather than individual ones, and pseudonyms such as "brouteur X", were preferred and the data collected were encoded.

Regarding data availability, the datasets generated and/or analysed during the study are available from the corresponding author upon reasonable request.

Analysis Strategy

Out of the total number of interviews conducted, seventeen were considered relevant based on interactions with cyberfraudsters, and eight with institutional actors. The exclusion of certain interviews was due to insufficient information collected during those sessions. However, these discussions offered a deeper insight into the management of proceeds originating from cyberfrauds and involvement in other forms of scams.

Qualitative content analysis was employed to categorise all the information gathered during interviews, both with *brouteurs* and institutional actors, into an analytical framework representing the discussed topics (Prior, 2014). Subsequently, a thematic analysis was

conducted to construct cross-cutting typologies of practices and representations (Blanchet & Gotman, 2005). The segmented themes of interest for this paper are the techniques used for receiving, spending, investing, and concealing cybercriminal proceeds, and the actors implicated in the fraudulent schemes.

Analysing these themes related to the management of cybercriminal proceeds is crucial, as this subject has been significantly underrepresented in existing literature. A study of this nature focusing on insights from the fraudsters themselves serves to draw attention to evasion mechanisms and gaps within the legal framework.

Limitations

The project's methodology presents several research limitations that are inherent to the topic, and it is advisable to take preventive measures for the design of future studies. Difficulties arose during the adaptation and understanding of interaction dynamics, initially reducing the study's effectiveness. During the initial weeks, the team primarily adopted an observational strategy to guard against team experience biases. Research planning was approached cautiously based on information gathered from the people encountered.

Furthermore, cybercriminals generally operate in secret, despite their visibility, leading to challenges in establishing reliable contacts and obtaining cooperation from various actors. In addition to the challenge of reaching them, as Levi and Soudijn (2020) highlight: "talking about money is much more dangerous than talking about past misdeeds (…)" (p.16). Precautions were therefore taken to not compromise the security of the interviewers and the interviewees, such as the presence of a local resource person that helped, as a key informant, reduce exposure and approach each situation with caution.

The number of interviews conducted represents another methodological limitation because while the gathered information is relevant to the subject theory, it does not allow for definitive conclusions regarding a relatively little-known phenomenon.

The sensitivity of the topics discussed and the interview locations may elicit reluctance from cybercriminals to share information or experiences, and could even lead to a premature termination of interviews due to fear of betrayal or retaliation with the other members of their networks. This might restrict access to authentic interviews. In this context, when encountering hesitation or non-responses to certain questions, interviewers aimed to continue the conversation without focusing on these gaps. Additionally, meeting locations were determined in collaboration with the participants to create an environment conducive to trust and, if necessary, shielded from prying eyes.

Lastly, this contribution seeks to be as detailed as possible to provide insights into the specific context in which the research was conducted (Ayerbe & Missonier, 2007).

Results

How cybercriminals receive the criminal proceeds?

The interviews provided insights about the evasion mechanisms employed by Ivorian cyberfraudsters regarding how they receive criminal proceeds. The *brouteurs* acknowledge that, even if they are the operational agents of the scams, targeting victims and extorting

money from them, they do not work alone. "Everyone is part of a network"[1], some *brouteurs* explain. Individuals engaged in the money-receiving strategies, and whose tasks are explained in Table 1, play a pivotal role in aiding the obfuscation of the money flow and in achieving the result of the scam, which is obtaining the money.

Fraudsters rely on what they term "*buralistes*", who could be referred to as professional middlemen or underground bankers. "These are, often, people who have good knowledge of financial circuits and offer their services to withdraw our money" explained an interviewee. These economic operators offer withdrawal services at transfer agencies, exchange prepaid cards, and direct bank transfers within Côte d'Ivoire and other African, European, or American countries. For the majority of *brouteurs*¸ "It is mandatory to go through a *buraliste*". This is especially important since the targets are abroad and "it's when you don't have anyone abroad that you are forced to go through a *buraliste*". Once the money from the scam is retrieved, these middlemen redistribute the funds in cash to network members. If the *buraliste* is part of a fraudster network, he usually retains 20% of the gain amount. If the *buraliste* is new to the network or operates independently, the request can reach 30–50% of the amount. These intermediaries make their availability known to fraudsters primarily through instant messaging platforms, such as WhatsApp status updates or social media.

Almost all the interviewed fraudsters mentioned the involvement of "accomplices": individuals from their neighbourhoods but mostly from the diaspora. They facilitate the process by making their bank accounts available for transfers, withdrawals, cash transfers, or other means to send money. "There is always someone there who takes all the deposits; they also have the French accounts", said an interviewee, explaining the need for contacts with French phone and bank accounts for the smooth operation of their scam. While not explicitly labelled as such by the fraudsters, these individuals essentially carry out the tasks of financial mules. In return for their services, they regularly receive a percentage, ranging from 10 to 30%, which helps them rationalise their availability when in difficult financial times and incentivises them to maintain a favourable relationship with the fraudsters.

Furthermore, *brouteurs* also admit to corrupting agents, such as police officers, bank personnel, or transfer agency staff, to facilitate the opening of accounts and with the withdrawal of money without proper identification, to turn a blind eye to falsified documents, or to avoid reporting suspicious or criminal activities to the relevant authorities. A *brouteur*, for example, indicates that "We always work with public agents. If they know you, it's easy; that's why I always have a contact in agencies and banks". Another provides more details about the nature of these relationships: "I also work with public agents: bank employees, doctors, law enforcement officers, pharmacists, real estate agents, and car dealers. All of them help either facilitate money withdrawals without suspicion, obtain fake documents, create fake companies, or facilitate the transport of money." These agents willingly neglect their duty and help facilitate criminal activities in exchange for varying amounts of bribes.

The cyberfraudsters offer their victims various means to send money with the involvement of different actors whose roles are described in Table 1. Firstly, as explained in Table 2, they suggest transferring money through various money transfer services like Western Union, Money Gram, Ria, etc. An interviewee describes his point of view: "All methods work. Often, it is the client who suggests the method based on their availability. But transfer agencies are the most popular." The collection is carried out by someone working within the service, an accomplice, or a *buraliste*, in exchange for a percentage of the obtained amount.

[1] All quotes have been translated by the authors from French or Nouchi into English.

Table 1 Individuals involved in the reception of cybercriminal proceeds

Ivorian cybercriminal network members	Members' tasks
Brouteurs	Cyberfraudsters or operational agents of cyberscams, their task is to establish contact with victims and extort money from them.
Buralistes	Professional middlemen and economic operators of cyberscams, they offer withdrawal or transfer services through banks, transfer agencies, prepaid cards or other means through Ivorian, African, European or American countries.
Accomplices	Neighbours, friends, acquaintances, or members of the diaspora engaged by *brouteurs*, theys make their accounts available for transfers, withdrawals, or other means of moving or sending money.
Corrupt agents	Police officers, transfer agency staff or bank personnel, theys facilitate the fraud process at most steps where public institutions are involved.

Table 2 Means used by cyberfraudsters to receive the illicit proceeds

Means to receive the cybercriminal proceeds
Transfer agency
Bank transfers
Prepaid cards
Mobile money transactions
Crypto wallet
Online payment services
Fake companies

Secondly, equally favoured are bank transfers to accounts held by money mules, acquaintances, or other individuals within the network, potentially using fake identities or identities of other scam victims. These transfers, along with their withdrawals, are often staggered to avoid raising suspicions with authorities by exceeding certain amounts. A *brouteur* explains using the method: "We don't withdraw everything at once; we take out half and send it little by little."

The use of prepaid cards like PCS, Neosurf, and others, as well as electronic mobile money transactions, are also possible, with the recipients not necessarily being the actual users of the money. It is this very case in this story: "Since you want to withdraw your money, you talk to the scammers, who recommend people who withdraw it for you". Indeed, this strategy prevents exposing the individual, who doesn't identify as a scammer personally, to risks by using accomplices. To a lesser extent, the fraudsters offer cryptocurrency wallet addresses or online payment services like Paypal, UBA Africash, Small World, Sigue, Wari, and others.

Stakeholders involved in combatting money laundering and cybercrime also provide insights into the mechanisms of receiving illicit funds. In addition to corroborating the statement of cyberfraudsters, they add that the latter use European, American, or African accounts of money mules to facilitate the flow of money and obfuscate its trace. Cyberfraudsters also employ accounts and documentation from fake companies, such as fake real

estate agencies, to make victims, mules, or financial intermediaries believe in the legitimacy of their scheme. Anti-money laundering actors highlight the significant role of corruption in cybercrime, represented as a substantial element for receiving, but also for laundering money and concealing evidence. "[They] (*brouteurs*) have contacts in institutions, whether in banks, police, security guards, or [transfer] agencies. One doesn't necessarily use fake documents because the person who withdraws is part of the network", complicating the detection and disruption of *brouteurs'* activities.

How the cybercriminals spend and invest the criminal proceeds?

Once the money is in their possession, the cyberfraudsters have various ways of spending it, without a specific preference, as described in Table 3. They often use the money to improve their living conditions, as well as to show off and make a splash, buying branded clothing, cars, and impressing their friends and romantic interests. The proceeds are also used for family expenses and daily expenditure. For instance, a *brouteur* said: "Often, if we do this, it's for the fame that comes from a need to fill a void compared to other friends. It's also to follow the trend, (…), at first, it's definitely just for show". Another one explained that he usually spends his money in more discreet manner: "The money I earn is mainly for the whole family. Both my parents are no longer here, and I am the eldest. So I use some of it for housing, food, and the schooling of my younger siblings."

The statements of institutional actors confirm again those of the scammers. In the cases encountered, the fraudsters primarily spend their money on everyday life expenses and the show business in general. The interviewed actors explain that, according to their observations, "The reintroduction of the money primarily occurs at night, especially in show business, to make a big splash". They are highly demonstrative with their earnings, often indulging and partying, spending on gifts for women and travel expenses. Furthermore, they assist acquaintances and neighbours by distributing a portion of their gains, contributing to financial education, or providing school kits for instance. "The scammer are happy because they can redistribute", and it's also a way to justify their actions and perpetuate a positive social perception of illicit activities.

Illicit funds are often used to enhance criminal methods (Table 4), such as purchasing phones, computers, or strengthening their network relationships (cybercafé proprietors, middlemen, IT specialists, etc.). A participant illustrates this through the following statement: "I spend a lot in daily life, but I invest in equipment to be able to excel in the field of crime." This other scammer has another strategy: "Others spend on clothes, bars, restaurants, but I prefer to invest in upscale bars, clothing stores, and show shops to avoid hardship later on." Similarly, other fraudsters also invest in opening small businesses such as transportation services, cybercafés, money transfer sub-agencies, cosmetic products, phone booths, and local eateries, aiming to increase their profits and distancing themselves from cybercriminal activities. Most of the participants view scamming as a temporary occupa-

Table 3 Means used by cyberfraudsters to spend the illicit proceeds

Means to spend the cybercriminal proceeds
Daily expenses
Putting on shows, partying
Luxury clothing and cars
Distribution to family and the community

Table 4 Means used by cyberfraudsters to invest the illicit proceeds

Means to invest the cybercriminal proceeds
Enhancing cybercriminal methods
Opening small businesses
Transportation
Car resale and rental
Car washing
Restaurants, local eateries
Cybercafés
Cosmetic products
Sub-agencies for fund transfers
Buying land
Constructing buildings, houses, or mines
Import-export businesses

tion, a means to make quick money. "I'll hustle until I make enough money; not being *hurt*[2] anymore is the main reason", explains one interviewee. "As soon as I have enough money, I'll stop; hopefully, that will be within five years", tells another. They also channel their investments into real estate, building houses, or even establishing mining ventures to secure their future family life. A detained *brouteur*, for example, describes his wealth: "I have gold mines in Bouaké, I've invested in friends' shops, and I want to build houses." In this way, they ensure a certain level of financial security for their families, partners, and friends, in a society where pursuing professional education and securing employment is challenging.

In addition, in cases observed by the interviewed anti-cybercrime and anti-money laundering actors, fraudsters invest in small businesses such as vehicle resale and rental, car wash services, catering or money transfer operations that aid other scammers in carrying out their activities. Several actors explained: "The channels for money laundering and reinvestment include the resale and rental of cars, small businesses, bars, night clubs, events, car washes, as their turnover is cash." Cyberfraudsters also venture into import-export businesses, maintain international connections through the cybercriminal network.

The interviewed cybercriminals didn't seem much preoccupied with the concealment of their gain. The amounts they obtain usually involve enough actors and transactions, so that the paper trail is lost, and the money laundering is realised.

Discussion and Conclusions

Cybercriminals are drawn to the characteristics of the internet, which also lead them towards cyberscams. These characteristics pose significant obstacles to the fight against these activities, including anonymity, the absence of face-to-face contact, transaction speed, globalisation processes such as free movements of goods, services, people, new payment technologies, and cross-border activities (Nizovtsev et al., 2021). The fraudsters employ legal circumvention mechanisms and deviant practices right from the outset of their scheme, obfuscating trails for investigations. They conceal identities behind fake names or pseudonyms, use VPNs or proxy servers. They may also employ false documents, featuring stolen or altered credentials, and use coded languages and data protection systems (Odinot et al., 2017).

The present study attempted to address the following question: What strategies do Ivorian cyberfraudsters use to manage and launder the criminal proceeds? These techniques form the

[2] « Poor » in *nouchi*.

basis for circumventing the law, which seeks to contain the phenomenon of cybercrime, as well as all its underlying but necessary aspects, such as money laundering. Indeed, money laundering, although an integral part of a scam script, is crucial for achieving the ultimate goal and deserves particular attention. The actors in both phenomena work closely together, and preventing their cooperation could significantly reduce cybercrime (Levi, 2015; Lusthaus et al., 2023).

The fight against money laundering seems to have a solid legal foundation in Côte d'Ivoire: Law No. 2016−992 concerning the fight against money laundering and the financing of terrorism allows for the identification of the actors and punishable acts. In this sense, anyone who has participated in the process of concealing the origin of assets derived from criminal activities or who has accepted such assets, suspecting that they are criminal proceeds, could be subject to punishment. Law 2016 also imposes obligations on all financial intermediaries, such as banks and affiliated mobile money issuers, as well as money transfer agencies. As a result, financial intermediaries are required to report their suspicions to the CENTIF by monitoring money transfer amounts and justifications, for example. Financial intermediaries have control mechanisms stipulated by the law, and the CENTIF and West African Monetary Union (WAMU) ensure the compliance of their activities.

Given the numbers of suspicious transaction reports and the increasing numbers of cybercrime, there may be a gap linked to "how the [anti-money laundering] regime is actually put into practice" (Levi & Soudijn, 2020, p.26). The interviewed institutional actors appear to be aware of the methods that cybercriminals use to recover illicit money. This could be a matter of their capacity (or willingness) to respond to these strategies and prevent them. The interviewed actors also point out the lack of personnel, training, and resources for detection and investigation, prolonging investigations against cybercriminals, money launderers, and potentially corrupt personnel.

The issue does not seem to be exclusive to Ivorian authorities. On the contrary, it is a recurring issue in international literature, as the money laundering strategies seem to be, with an adequate solution still to be found. A recent report of the Financial Action Task Force (2023) enumerates some successful strategies against cyber-enabled frauds and the illicit financial flows emanating from it: outline the responsibility and coordination of investigations, establish dedicated units for cybercrimes and money laundering, make financial information accessible, and deter financial mules. However, none of this is possible if each institution and individual pursue their own interests and work without synergy.

All the interviews conducted indicate the involvement of accomplices in the process of receiving and spending the money. The division of labour and professionalisation of services also appear to be part of strategies to circumvent the law. While network organisation primarily enhances their gains and efficiency (Azi, 2021), it allows the *brouteurs* to efficiently use each member's skills and services, all working toward the common goal of enrichment. According to the results of the present study, Ivorian cyberfraudsters' networks seem to rely on the same organisation as Leukfeldt (2014) identified in his study on Dutch phishing scam networks: in addition to core members who initiate the scam, the latter also engage professional enablers, recruited enablers, and money mules. Professional enablers are individuals who offer services such as fake documents or the development of phishing websites. Recruited enablers possess crucial information or resources for the execution of criminal activities, and cybercriminals pay to obtain them. Finally, money mules provide their bank accounts for use, whether knowingly or unknowingly, and may or may not be compensated.

Transposed this dynamic to Ivorian cyberfraudsters, *brouteurs* can be considered as the core members of the scam, as they have the role of organising its execution and initiating the process. *Brouteurs* engage *buralistes* or professional middlemen, who offer their services for the smooth execution of cybercriminal activities and the reception of money. *Brouteurs* also work with corrupt public officials involved with banks, the police, money transfer agencies, and any other public institutions, who knowingly violate their professional duty in exchange for a percentage of the deal. Finally, *brouteurs* also use accomplices, witting or unwitting money mules, often local acquaintances, or members of the diaspora, to grease the wheels of their illicit activity. It is unclear from the realised interviews how easy or difficult it is to get these accomplices, or what are their intentions or the coercive factors that support their involvement. It is also unclear to what extent cyberfraudsters depend on these accomplices and how easy it is to get to them. Addressing these elements would help understand the coordination of illicit flows, as well as the efforts undertaken to circumvent anti-money laundering regulations.

Lusthaus et al. (2023) observed that malware and cyberfraud cybercriminal networks concentrate on converting the criminal proceeds into cash. The authors' findings indicate a clear distinction between cybercriminal network members and money laundering network members composed of a leader and money mules. The authors advise further research on money laundering networks, which do not confine their activities to the online realm but, conversely, employ relatively unsophisticated and well-known methods.

Ivorian cyberfraudsters use several strategies, indeed quite unsophisticated, that appear to be effective in allowing cybercriminals to evade the scrutiny of financial intermediaries and prosecution authorities. Firstly, they employ money mules and *buralistes* to transfer money between multiple bank or money transfer accounts, making it difficult to trace the money to them. Secondly, they divide money transfers into smaller sums to avoid arousing suspicion among financial intermediaries. This ancient technique is known as "smurfing" (Welling, 1989). It is even possible that cybercriminals establish their own money transfer sub-agencies, a practice accessible to almost anyone (AITN, 2022), to facilitate their own operations or those of their associates. Ivorian cyberfraudsters also forge false documents of fictional companies to open banks accounts, often with the assistance of individuals such as IT specialists and bank personnel, enabling the simplified transfer of larger sums without arousing suspicion. Furthermore, scammers cover their tracks by using their contacts working within financial intermediaries or by easily corrupting their personnel. *Brouteurs* directly withdraw the money transmitted to them by the *buralistes*, in order to avoid having it seized. Once the cybercriminals receive the proceeds, they spend it just as quickly as they received it and their trail is lost.

Brouteurs primarily receive their cybercriminal proceeds in cash because of the involvement of all these strategies. Only very few mention receiving and using cryptocurrencies, while others suggest they do not understand what virtual currency represents conceptually. It is entirely possible that the use of this technique to manage their assets will increase with the evolution and growing reputation of cryptocurrencies in Côte d'Ivoire, especially considering the opportunity that the lack of regulation regarding VASP could represent. However, it is quite unlikely that this will replace the money laundering strategies already in place, which are less sophisticated and sufficiently effective (Custers et al., 2019; McGuire, 2018; Nazzari, 2023; Paquet-Clouston et al., 2019; Soudijn, 2019).

These strategies, known as efficient and easy to set up for various forms of cybercrime and traditional crime, are well-documented in the literature (Akadje et al., 2018; Bekkers et al., 2023; European Police Office, 2015; Kramer et al., 2023; Kruisbergen et al., 2019; Odinot et al., 2017;

Trend Micro & Interpol, 2017; Weber & Kruisbergen, 2019). Furthermore, Ivorian cybercriminals would not currently need to enhance them, as even the "humblest" strategies remain undisturbed or unmitigated. Cyberfraudsters, as well as other types of (cyber-)criminals studied in empirical research from all over the world, seem to adjust their money management strategies based on the measures implemented in the fighting strategies (Levi, 2015; Levi & Soudijn, 2020; Nazzari, 2023). Similarly, cyberfraudsters, though they might employ offline activities in their online scams, wouldn't need to adapt their strategies in regard with the management of their money. Indeed, in cases of hybrid online or offline organised crime activities, offenders seem to have the same preference for unsophisticated methods of money laundering and for cash, as it seems also to be the case for the interviewed individuals (Kruisbergen et al., 2019).

This article adds to the existing literature on Ivorian cybercrime, specifically focusing on cyberfrauds. The study that gathered the information discussed in this paper has several limitations. The study represented the research team's first visit to Côte d'Ivoire regarding the subject, which required adaptation to the local environment and Ivorian lifestyle. This adjustment process led to a slower initiation of the study, further delayed by administrative and procedural steps that were time-consuming. The study managed to conduct a limited number of interviews, increasing this number could have provided a more comprehensive understanding of a rather complex phenomenon. Additionally, the interviews were conducted solely with *brouteurs*, who were operational actors in the scam but not with *buralistes*, complicit public officials, or money mules, who were operational actors in money laundering. The information described in this paper is therefore inferred from the statements of cybercriminals who work closely with those involved in criminal proceeds reception strategies, which may introduce certain biases.

To address these limitations, the research team advocates for the development of future research to continue expanding knowledge about these relatively underexplored phenomena in both academic and practical contexts. In general, the use of different methodologies beyond semi-structured interviews and a qualitative approach would allow for a multifaceted examination of cybercrime from various perspectives. This could include assessing the prevalence of cybercrime or cybervictimisation, understanding its spatial distribution in the West African region, investigating cybercriminal practices and money laundering, as well as varying strategies for combatting these issues across different countries in the region. The results could be analysed to describe the scripts of cybercrime, related money laundering, or the analysis of networks involving money laundering actors and their interactions with cybercriminal networks.

It would be of paramount importance for practitioners and national and international experts to prevent cybercriminals from profiting from criminal assets, to identify gaps and focus available resources on addressing these issues (Koffi & Soro, 2022; Mugarura & Ssali, 2020; Shaw & Reitano, 2020; van Vuuren et al., 2020 and all the authors mentioned in this article). In this regard, international police and judicial cooperation appear to warrant attention (van Vuuren et al., 2020). While not currently a priority, criminal intelligence has demonstrated its effectiveness in combating organised and networked crime (Odinot et al., 2017). Given the organised nature of cybercriminal and money laundering networks, it could be a functional response to combat this ongoing issue.

The present paper has shed light on the actors and means involved in the reception of criminal assets, including cybercriminals, professional middlemen, accomplices, money mules, as well as corrupt public agents who receive, transfer, and send money from victims through transfer agencies, bank transfers, prepaid cards, mobile money transactions, online payment services, or even crypto wallets. Typically, cyberfraudsters receive the money in cash, allowing them to avoid the

need for money laundering since money received in cash is already untraceable. Upon receiving the money, they spend it on daily expenses, parties, luxury clothing, cars, or distribute it to their families and communities. On the other hand, *brouteurs* invest their earnings to enhance cybercriminal methods, open small businesses, purchase, or construct properties, or engage in import-export businesses. These means enable them to envision a financially stable future, hoping to no longer resort to criminal activities to meet their needs.

The way they manage their money provides valuable insights into the mechanisms for circumventing the law. It underscores the fact that law enforcement alone is not sufficient to detect the criminal nature of their activities, or at the very least, the law is not effectively enforced to detect and prosecute these phenomena. This raises questions about the triangular relationship between cybercrime, money laundering, and corruption (as discussed in Richards & Eboibi, 2021 and GIABA, 2022). "Have you ever tried sweeping a staircase from the bottom to the top? No, because to get a good result, you need to start from the top." If the connections between two of these phenomena are broken, it is highly likely that this disruption will affect the link with the third. This deserves further attention and empirical investigation.

Acknowledgements The study was funded by the Leading House Africa programme of the Swiss Tropical and Public Health Institute, the Center for Development and Environment of the University of Bern and the University of Basel, mandated by the State Secretariat for Education, Research and Innovation of Swiss Confederation.

Funding Open access funding provided by University of Applied Sciences and Arts Western Switzerland (HES-SO)

Declarations

Compliance with Ethical Standards There are no potential conflicts of interest. The research involved human participants as interview subjects. Informed consent was obtained in all cases.

References

Abdul Rani, M. I., Mustapha Nazri, S., S. N. F., & Zolkaflil, S. (2023). A systematic literature review of money mule: Its roles, recruitment and awareness. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-10-2022-0243

Addo, P. (2006). Cross-border criminal activities in West Africa: Options for effective responses. *KAIPTC Paper*, *12*.

Adou, E. F. S. (2022). Les brouteurs d'Abidjan. *RESET Recherches en Sciences Sociales sur Internet*, *11*. https://doi.org/10.4000/reset.4038. /11.

Ahissan, A. K., Okpo, A. N., & Azi, J. W. (2017). Cybercriminalité et réseaux criminels à Abidjan. *Revue Internationale De Recherches et d'Etudes Puridisciplinaires*, *26*, 63–74.

AITN (2022). janvier 5). Voici comment ouvrir une agence de transfert d'argent en Côte d'Ivoire. AITN. URL: https://afriqueitnews.com/finance/voici-comment-ouvrir-agence-transfert-argent-cote-ivoire/

Akadje, M. A. (2011). Cybercriminalité Et « Broutage » à Abidjan. *Revue internationale de criminologie et de Police Technique et scientifique*, *3*, 299–310.
Akadje, M. A., Sahi, R. S., & Mouli, H. (2018). Utilisation Du Gain Issu Du « Broutage » à Abidjan. *International Journal of Current Research*, *10*, 76704–76713.
Akadje, M. A., Zady, C., & Azi, J. W. (2017). Parents et "Broutage" À Abidjan. *European Scientific Journal ESJ*, *13*(5), 285–302. https://doi.org/10.19044/esj.2017.v13n5p285
Aman, V. (2023). *Chantiers de la lutte contre la cybercriminalité en Côte d'Ivoire* (p. 50).
Atta-Asamoah, A. (2009). Understanding the west African cyber crime process. *African Security Studies*, *18*(4), 105–161.
Ayerbe, C., & Missonier, A. (2007). Validité Interne et validité externe de l'étude de cas: Principes et mise en oeuvre pour un renforcement mutuel. *Revue Finance Contrôle Stratégie*, *10*(2), 37–62.
Azi, J. W. (2021). Perceptions favorables de la Cyberescroquerie et des réseaux cyberescrocs Chez Des Jeunes à Yopougon. *Revue Africaine De Criminologie*, *28*, 66–81.
Bailey, J., Taylor, L., Kingston, P., & Watts, G. (2021). *Older adults and scams: Evidence from the mass observation archive*. https://doi.org/10.1108/JAP-07-2020-0030
Barnor, J. N. B., Boateng, R., Kolog, E. A., & Afful-Dadzie, A. (2020). Rationalizing online romance fraud: In the eyes of the offender. *AMCIS 2020 Proceedings*, *21*, 1–10.
Bazare, R. N., Ladji, B., & Kadidja, D. (2017). Cybercriminalité Ou « Broutage » Et crimes Rituels à Abidjan: Logiques Des Acteurs Et Réponses Au Phénomène Cas Des Communes De Yopougon et d'Abobo. *European Scientific Journal ESJ*, *13*(23), 104. https://doi.org/10.19044/esj.2017.v13n23p104
Bekkers, L., Van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Money mules and cybercrime involvement mechanisms: Exploring the experiences and perceptions of young people in the Netherlands. *Deviant Behavior*, *0*(0), 1–18. https://doi.org/10.1080/01639625.2023.2196365
Blanchet, A., Giami, A., Bézille, H., Florand, M. F., & Pagès, M. (1985). *L'entretien dans les sciences sociales: L'écoute, la parole et le sens*. Dunod.
Blanchet, A., & Gotman, A. (2005). In *L'enquête et ses méthodes: L'entretien*. Éds: Armand Colin, pp. 91–101.
Boateng, R., Olumide, L., Isabalija, R., & Budu, J. (2011). Sakawa – Cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, *11*(2), 85–100.
CENTIF (2013). Premier Rapport de Suivi de L'Evaluation Mutuelle de la Cote D'Ivoire. Octobre 2013.
Cross, C. (2023). "I knew it was a scam": Understanding the triggers for recognizing romance fraud. *Criminology & Public Policy*, 1–25. https://doi.org/10.1111/1745-9133.12645
Cross, C., Holt, K., & O'Malley, R. L. (2022). If U don't pay they will share the pics: Exploring sextortion in the context of romance fraud. *Victims & Offenders*, *0*(0), 1–22. https://doi.org/10.1080/15564886.2022.2075064
Custers, B. H., Pool, R. L., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. *European Journal of Criminology*, *16*(6), 728–745. https://doi.org/10.1177/1477370818788007
ECOWAS (2021). ECOWAS regional cybersecurity and cybercrime strategy. 2021.
European Police Office (2015). *Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering* Publications Office. URL: https://data.europa.eu/doi/10.2813/698364
FATF, Interpol, & Egmont Group (2023). *Illicit financial flows from cyber-enabled fraud*. FATF. www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/iIllicit-financial-flows-cyberenabled-fraud.html
Federal Bureau of Investigation (2021). Internet crime report. 2021.
Federal Bureau of Investigation (s. d.). *Dont' be a mule: Awareness can prevent crime* [Page]. Federal Bureau of Investigation. URL: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules
Fortin, F. (2013). (Éd.). Nouveaux habits de la vieille fraude: Une vision « écosystémique » des fraudeurs, de leurs instruments et de leurs victimes. In *Cybercriminalité: Entre inconduite et crime organisé*. Presses internationales Polytechnique et Sûreté du Québec.
GIABA. (2022). *Rapport de typologies de blanchiment de Capitaux et Financement Du Terrorisme é Travers La Corruption en Afrique de l'Ouest*. GIABA.
GIABA (2023). Anti-money laundering and counter-terrorist financing measures – Côte d'Ivoire, Second Round Mutual Evaluation Report, GIABA, Dakar. June 2023.
Grandjean, F., Cretu-Adatte, C., Beaudet-Labrecque, O., & Zbinden, R. (2022). Wenn aus Einem Opfer eines Romance Scams Ein Money Mule wird. *Kriminalistik*, *2022*(11), 1–6.
Gueu, D. (2013). La Cybercriminalité à Abidjan, Un Phénomène De Mode Ou une Nouvelle Guerre Contre Les Finances en Côte d'Ivoire? *European Scientific Journal*, *9*(1), 97–106.

Horgby, A., Särnqvist, D., & Korsell, L. (2015). *Money laundering and other money management. Criminal money, black money and murky money in the legal economy* (p. 10). The Swedish National Council for Crime Prevention.

Interpol (2021). African cyberthreat assessment. Interpol's key insight into cybercrime in Africa. Octobre 2021.

Interpol (2022). 2022 Interpol global crime trend summary report. Octobre 2022.

Koffi, H. B. D. I., & Soro, N. O. (2022). Stratégie De lutte contre la cybercriminalité en Côte d'Ivoire. *Revue Internationale Du Chercheur*, *3*(2).

Konan, K. P., Traoré, B. S., Ahounou, E. I., Ziketo, B. D. S., Aka, R. A., & Yeo-Tenena, Y. J. M. (2022). Cybercriminalité et occultisme chez des adolescents ivoiriens. *L'information Psychiatrique*, *98*(1), 41–47. https://doi.org/10.1684/ipe.2021.2370

Koné, Y. (2015). Le travail mondialisé du jour et le travaillement local la nuit. Journal des anthropologues. Association française des anthropologues. *Journal des anthropologues. Association française des anthropologues, 142–143*. 307–324. https://doi.org/10.4000/jda.6327

Kramer, J. A., Blokland, A. A. J., Kleemans, E. R., & Soudijn, M. R. J. (2023). Money laundering as a service: Investigating business-like behavior in money laundering networks in the Netherlands. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09475-w

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, *42*(5), 569–581. https://doi.org/10.1080/0735648X.2019.1692420

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in Organized Crime*, *17*(4), 231–249. https://doi.org/10.1007/s12117-014-9229-5

Levi, M. (2015). Money for crime and money from crime: Financing crime and laundering crime proceeds. *European Journal on Criminal Policy and Research*, *21*(2), 275–297. https://doi.org/10.1007/s10610-015-9269-7

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime Law and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime and Justice*, *49*, 579–631. https://doi.org/10.1086/708047

Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime DOI*. https://doi.org/10.1007/s12117-022-09476-9

McGuire, M. (2018). *Into the web of profit: Understanding the growth of the cybercrime economy* (p. 178). Bromium, Inc.

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28. https://doi.org/10.1108/JMLC-11-2019-0092

Nazzari, M. (2023). From payday to payoff: Exploring the money laundering strategies of cybercriminals. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09505-1

N'Guessan, A. (2014). La Pratique De La Cybercriminalité en Milieux Scolaire Et Universitaire de Côte d'Ivoire. Cas d'Elèves Du District d'Abidjan. *European Scientific Journal*, *10*(31), 178–195.

Nizovtsev, Y. Y., Parfylo, O. A., Barabash, O. O., Kyrenko, S. G., & Smetanina, N. V. (2021). Mechanisms of money laundering obtained from cybercrime: The legal aspect. *Journal of Money Laundering Control*, *25*(2), 297–305. https://doi.org/10.1108/JMLC-02-2021-0015

Odinot, G., Verhoeven, M. A., Pool, R. L. D., & de Poot, C. J. (2017). *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. WODC.

O'Malley, R. L., & Holt, K. M. (2022). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of Interpersonal Violence*, *37*(1–2), 258–283. https://doi.org/10.1177/0886260520909186

Paquet-Clouston, M., Romiti, M., Haslhofer, B., & Charvat, T. (2019). Spams meet cryptocurrencies: Sextortion in the Bitcoin Ecosystem. *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, *76-88*. https://doi.org/10.1145/3318041.3355466

Prior, L. (2014). Content analysis. *The Oxford handbook of qualitative research* (p. 785). Oxford University Press.

Richards, N. U., & Eboibi, F. E. (2021). 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), 131–161. https://doi.org/10.1080/13600869.2021.1885105

Richet, J. L. (2013). *Laundering money online: A review of cybercriminals methods* (arXiv:1310.2368). arXiv. https://doi.org/10.48550/arXiv.1310.2368

Shaw, M. S., & Reitano, T. R. (2020). Organized crime and criminal networks in Africa. *The Oxford Encyclopedia of African Politics*. Oxford University Press. https://www.oxfordreference.com/display/https://doi.org/10.1093/acref/9780190632342.001.0001/acref-9780190632342-e-742

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*(3), 342–361. https://doi.org/10.1057/s41284-019-00166-w

Soudijn, M. R. J. (2019). Using police reports to monitor money laundering developments. Continuity and change in 12 years of Dutch money laundering crime pattern analyses. *European Journal on Criminal Policy and Research*, *25*(1), 83–97. https://doi.org/10.1007/s10610-018-9379-0

Tasso, B. F., & Ouassa Kouaro, M. (2014). La cybercriminalité Au Bénin: Une étude Sociologique à partir des usages intelligents des technologies de L'information et de la communication. *Les enjeux de l'information et de la Communication*, *15*, 35–42.

Trend, M., & Interpol (2017). *Cybercrime in West Africa: Poised for an underground market*. *Interpol*, *34*.

van Vuuren, J. J., Leenen, L., & Pieterse, P. (2020). Development and implementation of cybercrime strategies in Africa with specific reference to South Africa. *Journal of Information Warfare*, *19*(3), 83–101.

Wang, F., & Topalli, V. (2022). Understanding Romance scammers through the Lens of their victims: Qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-022-09706-4

Wannenburg, G. (2005). Organised Crime in West Africa. *African Security Review, 14*(4), 5–16.

Weber, J., & Kruisbergen, E. W. (2019). Criminal markets: The dark web, money laundering and counterstrategies - an overview of the 10th research conference on organized crime. *Trends in Organized Crime*, *22*(3), 346–356. https://doi.org/10.1007/s12117-019-09365-8

Welling, S. N. (1989). Smurfs, money laundering, and the Federal Criminal Law: The crime of structuring transactions. *Florida Law Review*, *41*, 287.

Yin, R. K. (2011). *Qualitative research from start to Finish*. Guilford Press.

Authors and Affiliations

Cristina Cretu-Adatte[1] · Renaud Zbinden[1] · Luca Brunoni[1] · Hazel Bunning[1] · Josselin Wilfred Azi[2] · Olivier Beaudet-Labrecque[1]

✉ Olivier Beaudet-Labrecque
olivier.beaudet-labrecque@he-arc.ch

Cristina Cretu-Adatte
cristina.cretu-adatte@he-arc.ch

Renaud Zbinden
renaud.zbinden@he-arc.ch

Luca Brunoni
luca.brunoni@he-arc.ch

Hazel Bunning
hazel.bunning@he-arc.ch

Josselin Wilfred Azi
ajosselinwilfred@gmail.com

[1] Institute of Economic Crime Investigation (ILCE), HEG Arc // HES-SO, Neuchâtel, Switzerland

[2] Department of Criminology, University of Félix Houphouët Boigny UFHB, Abidjan, Ivory Co ast