International Journal of Law, Crime and Justice 84 (2026) 100825

Contents lists available at ScienceDirect

International Journal of Law, Crime and Justice

journal homepage: www.elsevier.com/locate/ijlcj

Evolutionary fraud, the global scamming ecosystem and a typology of actors

Mark Button [a,*], Suleman Lazarus [b,e], Branislav Hock [a], Paul Gilmour [a], Durgesh Pandey [c], James Bugbilla Sabia [d]

[a] University of Portsmouth, UK
[b] London School of Economics and Political Science (LSE), UK
[c] Gujarat University, India
[d] Ghana Armed Forces, Ghana
[e] University of the Western Cape, Cape Town, South Africa

ARTICLE INFO

Keywords:
Geography of crime
Scamming ecosystem
Cybercrime typology
Transnational organized crime
Fraud typology
Scamvolution
Cyber criminology

ABSTRACT

This study examines the adaptive nature of the global scamming ecosystem, focusing on developing a novel typology based on the size and organizational structure of scam operations. Through a combination of qualitative and case study analysis, the research categorizes scammers into five distinct groups, namely, "Demons," "Gorgons," "Ogres," "Behemoths," and "Mega Behemoths," ranging from lone actors to large-scale enterprises with intricate hierarchies and international reach. The findings highlight how organizational size, specialisation, and corrupt actors' involvement contribute to scam operations' effectiveness and resilience. Findings also illustrate the adaptive processes observed in legitimate business practices, including role specialisation and hierarchical organization strategic planning. The paper also notes the evolutionary processes creating more effective scams and means of delivering them. The study provides a foundational understanding of these dynamics, offering a framework for targeted, flexible strategies and robust international cooperation. Findings also highlight the importance of continued interdisciplinary collaboration to address these evolving threats.

1. Introduction

The global scamming ecosystem has evolved significantly into a highly complex, multi-billion-pound industry (e.g., Engle et al., 2015; United Nations, 2023). It encompasses a wide range of actors, from individuals barely making a subsistence living through fraudulent activities to highly organised, large-scale enterprises that generate millions of dollars and employ thousands (Ferrante and Holt, 2025; Franceschini et al., 2023, 2025, 2024; Hall et al., 2021; Hall and Yarwood, 2024; Lazarus, 2024; United Nations, 2023). The scale and sophistication of this ecosystem mirror those found in legitimate sectors, characterised by diverse organisational structures and specialised roles, the growth of which has been described as an "industrialisation" (Lazarus et al., 2026; Wang and Topalli, 2024a). These structures and roles have developed through an evolutionary process, one that is driven by the pressures of law enforcement, anti-scam actors, technology, competition among fraudsters, and the relentless pursuit of success (cf. Shover et al., 2004).

* Corresponding author.
E-mail addresses: mark.button@port.ac.uk (M. Button), suleman.lazarus@gmail.com (S. Lazarus), branislav.hock@port.ac.uk (B. Hock), Paul.Gilmour@port.ac.uk (P. Gilmour), durgesh.pandey@nfsu.ac.in (D. Pandey), bugdek@gmail.com (J. Bugbilla Sabia).

https://doi.org/10.1016/j.ijlcj.2026.100825
Received 11 March 2025; Received in revised form 15 December 2025; Accepted 16 January 2026
Available online 25 February 2026

This continuous adaptation, akin to natural selection, has resulted in a dynamic and ever-changing landscape of scamming tactics and organizational configurations.

Despite its far-reaching implications, comprehensive research on the global scamming ecosystem and the diverse range of actors within it remains limited (Andoh-Baidoo et al., 2024; Franceschini et al., 2023; Franceschini et al., 2024; Hall and Yarwood, 2024; Lazarus, 2024; Wang and Topalli, 2024a). This study aims to address this gap by proposing a detailed typology that categorizes scam operations based on their size and organizational structure. This typology, ranging from small-scale local scams to complex multi-national enterprises, serves as a framework to better understand the variety and dynamics of scamming activities. Moreover, the study introduces the concept of "evolutionary fraud," which captures the adaptive nature of scam operations as they respond to external pressures, such as technological advancements and heightened law enforcement measures. These operations, much like legitimate businesses, adopt specialized roles, hierarchical structures, and strategic planning, enhancing their effectiveness and resilience.

A significant dimension of this ecosystem is the role of corruption in sustaining scam operations. Corrupt actors, including law enforcement officials, politicians, and insiders within legitimate sectors, often provide protection, insider information, or even direct involvement, complicating efforts to combat these activities. In some parts of the world such as Cambodia and Myanmar political elites offer protective umbrellas for operators in return for a share of the profits (cf. Franceschini, 2024; Lazarus et al., 2026; Loughlin, 2024). Such systemic corruption not only facilitates the proliferation of scam networks but also highlights the intertwined nature of legitimate and illegitimate sectors. Furthermore, the study explores the cultural dimensions of scamming, particularly in West African contexts where supernatural beliefs and practices, such as juju magic, are integrated into fraudulent schemes (cf. Aransiola and Asindemade, 2011; Button et al., 2025; Lazarus, 2019; Lazarus and Okolorie, 2019; Yushawu and Jaishankar, 2025). These cultural elements, rarely observed outside African diaspora communities, underscore the need for culturally sensitive strategies in addressing these issues.

This article begins by reviewing the existing literature on organized fraud and cybercrime, identifying key gaps and underexplored areas. The methodology section follows, outlining the research approach and analytical framework employed. The findings are presented in three sections: the first categorizes scam operations by size and structure, providing a clear typology; the second examines specialized roles and strategies, supported by detailed case studies that illustrate the adaptive nature of these operations; and the final section discusses the role of corrupt actors and the influence of cultural nuances on scamming tactics. By presenting a structured typology and emphasising the dynamic and adaptive nature of scam operations, this study contributes to a deeper understanding of the global scamming ecosystem. It highlights the urgent need for targeted, culturally informed prevention strategies and robust international cooperation to effectively address these complex and evolving threats.

2. Literature review

Fraud is very broad in scope and encompasses an employee fiddling their expenses through to a gang phoning up random individuals trying to sell false investments. The scope of this paper is what some would call scamming or to be precise frauds that target individuals and organisations by external actors. It includes phishing scams that seek to secure sensitive personal information, romance scams and consumer frauds to name some, the vast majority of which are pursued online in some way. Beals et al. (2015) provide a comprehensive classification of the variety of scams, and Button and Cross (2017) add a further dimension by incorporating identity fraud. These categories are listed below.

- Consumer Investment Fraud
- Consumer Products and Services Fraud
- Employment Frauds
- Prize and Grant Fraud
- Phantom Debt Collection Fraud.
- Charity Fraud.
- Relationship and Trust Fraud
- Identity Frauds (Beals et al., 2015; Button and Cross, 2017: p 11-12).

Fraud has become one of the most common crimes in many countries (UNODC, 2024). A recent cross-country comparison of 15 countries found the fraud victimisation among the adult population in the years 2021-23 ranged from 31 % in the USA to 8 % in Japan, with another 9 countries experiencing victimisation rates above 20 %. This amounts to 228 million victims over the duration of the study or 76 million per year (Hyde and Gibson, 2024). The scale and cost of this problem has been estimated by the Global Anti-Scam Alliance to amount to be over $1trillion in losses, from over 2 billion victims with only 0.05 % of scammers caught (GASA, 2024). There is also strong evidence that a significant volume of fraud is cross-border. In the UK, the City of London Police has estimated that 70 % of frauds in England and Wales either originate from abroad or have an international element (Home Office, 2023, p.11).

There is a growing body of research on cybercriminals (which is a very broad concept, encompassing hackers, online abusers, and some cyber-fraudsters) (Ferrante and Holt, 2025; Ibrahim, 2016; Lusthaus et al., 2023; Smirnova et al., 2025; Soares et al., 2025), Nigerian scammers (Aransiola and Asindemade, 2011; Auwal and Lazarus, 2025; Lazarus et al., 2025; Lazarus and Okolorie, 2019) and South East Asian scam compounds (Franceschini et al., 2023; Lazarus et al., 2026). There have, however, been virtually no typologies

of scammers, although there have been of the methods and detailed descriptions of their structures (see for example Andoh-Baidoo et al., 2024; Lazarus and Okolorie, 2019; Lusthaus et al., 2025; Wang and Topalli, 2024b). One of the few is Levi (2008), who conducted research on long firm fraudsters. Long-firm fraudsters set up businesses and build up credit, gradually ordering more goods and eventually disappearing, not paying the debts. The scam is orientated more at organisations than individuals, although it could affect the latter. In conducting this research, Levi distinguished three useful categories of fraudsters, which are likely relevant to some mass marketing fraudsters (Levi, 2008). These are.

- **Slippery slope**: generally have no prior convictions and fall into frauds through pressures combined with identification of opportunities.
- **Intermediate long firm fraudsters**: some with prior convictions who started off with legitimate intentions, but eventually turn to fraud.
- **Pre-planned long firm fraudsters**: the perpetrators typically begin with the intention to commit fraud and often have prior criminal convictions, although they may use 'front' individuals without convictions. Some may be involved in organised crime in the 'traditional' sense, such as drugs or racketeering, or have links to such activities, while others may focus solely on specific types of fraud.

Another useful typology to note, although covering workplace offending is the typology of 'cheats at work' developed by Mars (2019) to explore workplace deviance such as theft, fraud etc built upon their degree of autonomy and individual or group orientation. Mars used Hawks (who operate individually with autonomy such as academics, journalists), Donkeys (are subordinate in the organisation but operate solo, such as shop checkout staff), Vultures (operate individually but within bureaucratic structures, such as sales reps, couriers) and Wolves (groups who operate autonomously and independently such as aircrews, hospital staff) to describe different types of workplace cheats. This paper will later seek to develop a typology of scammers operating across the globe rooted in their size and organisational structure.

3. Methods

This article arose from a project commissioned to explore fraudsters active in Nigeria, Ghana and India. As part of that project, the researchers undertook a literature review and, using cases in the public domain, built a database of fraudsters in those countries who had either been convicted, indicted or had been interviewed by journalists. This produced a database of 97 fraudsters in those countries. This database was designed to capture key fraudster types and to illustrate the diversity and not capture all cases, which would have been time-consuming and offered little more in generating new knowledge about even more fraudsters of a similar type in the public domain. So once a particular type of fraudster was added, if there were recurring cases of a similar profile, the researchers would move to exclude any further cases. Indeed, in Nigeria, the Economic and Financial Crimes Commission (EFCC) annually publishes a list of successful prosecution cases which amounts to a few thousand each year. Many of these are similar young males from urban areas undertaking relatively low-level romance scams. It would have been pointless to populate this database with thousands of these similar cases. The wider literature also led to the identification of a number of sources that took a broader view than these three countries, particularly related to South East Asian scam compounds. The project also included interviews with a wide range of stakeholders with knowledge and expertise of this area, some relevant to one of the specific countries, some more widely. These included: law enforcement, government officials, academics, scamfighters (persons working individually to tackle fraud, some known as scambaiters), workers for NGOs operating in this sphere, as well as actual fraudsters. Table 1 illustrates the variety of interviews undertaken for this project. All interviews and data collection were undertaken according to usual ethical protocols.

Table 1
Range of interviewees.

Role	All (Multiple Countries)	Ghana	Nigeria	India
Government Officials	2	1	–	–
Academics	2	–	–	–
Law Enforcement	2	6	5	1
Scamfighters	5	–	–	–
Fraudsters	–	1	4	3
Cyber Expert	–	–	1	–
Consultant	1	–	–	1
NGO Workers	–	–	4	–
Member of Parliament	–	1	–	–
Prison Officer	–	–	1	–
Journalist	–	–	1	–
Total Respondents	**10**	**11**	**15**	**7**

4. Findings

This paper now illustrates the diversity of bad actors engaged in pursuing the wide range of frauds identified earlier in the literature review. This first section considers their size and organisational structures. Because many fraudsters operate in business like ways, the size based framework used to classify business organisations provides the basis for this typology. It ranges from loners, or sole traders, operating alone, through to large enterprises conducting fraud on an industrial scale, illustrated in Fig. 1.

This section will illustrate the range in size of scammer operations. It is important to note in the examples used one cannot always be confident of the facts. A convicted fraudster who says they worked alone might be protecting an accomplice(s). The size of a group reported for the same reason might not be accurate. Some groups that have been indicted also have a large number of actors, but whose members' depth of involvement may vary significantly. For instance, there might be listed a large number of money mules, whose only role is to simply accept and move a payment. These are not core members of a fraud enterprise. The same could be said of pyramid schemes, which technically all members are bad actors as they are trying to recruit 'victims', but who in reality are victims too with the ring leaders and organisers the real culprits (Beek, 2020; Hock and Button, 2023; Suwitho et al., 2023). We have therefore tried to be careful to investigate the numbers involved and focus on active and deeply involved participants. So, the facts of these cases should be considered as best available estimates and the purpose of the section is to use the best available evidence to illustrate the varying size and structure of bad actors operating in the scam ecosystem. Fig. 1 provides the range of size of scamming operation from lone person scammers through the very largest. We have utilized widely used classifications of different sized business enterprises and applied them to the findings on scammers (European Commission, n.d.). Additionally, we have termed these categories with mythical wicked creatures of varying size to further distinguish this typology.

4.1. Demons

Demons are bad actors that work predominantly alone. One of the scammers interviewed from Ghana fitted this category, who explained:

> I am alone. I do it alone, I don't know any others … I learnt it on my own … I was scammed by someone he wanted to hack my account … that's why I started all this kind of stuff (Ghana Scammer 1).

An investigator from Ghana noted that in his view most fraudsters worked alone or in very small groups in his country:

> Most of them are individuals and in some cases, they operate as syndicates of 4 members (Ghana Investigator 1).

Similarly, a law enforcement officer based in South Africa focused on combatting fraud in West Africa, thought the dominant size was loners or very small groups:

> … we do find that in the Ivory Coast as well as in Nigeria, it's it's more lone rangers working … (Law Enforcement South Africa).

A search of cases of fraud reveals many confirmed fraudsters who work alone. Like any sole trader there might be occasions where they need the support of others, but in this category the bad actor develops the scam alone, implements it and secures all the loot from the activity (minus any fees they may have to pay to those supporting their activities). All over the world cases can be found of individual scammers working alone in a wide range of different types of fraudulent enterprise targeting individuals and organisations. Some will target those in their own country from their own country, others will travel to other locations to target their own country – hoping this makes law enforcement activity less likely and some will simply target other countries. Some will act completely alone, others use the services of others to support their work – like any legitimate sole trader might do. There are many of these lone actors to be found in the media and the following illustrate some of the diversity of these cases.

In one case from the Nigerian Economic and Financial Crimes Commission, Adewale Tosin was convicted of defrauding an American man of $2400 while pretending to be a female with the name Zielone Nyson (Guardian, 2021). Some cases of individual

Sole Traders **Demons**	**Micro** **<10** **<€2m** **Gorgons**	**Small** **<50** **<€10m** **Ogres**	**SME** **<250** **<€50m** **Behemoths**	**Large** **>250** **>€50m** **Mega Behemoths**
Everywhere	Everywhere West African Yahoo Boys/ Sakawa Boys/ Brouteurs	Indian Call Centres West African Yahoo Boys/ Sakawa Boys	Indian Call Centres SE Asian Scam Compounds	Indian Call Centres SE Asian Scam Compounds Nigerian Confraternities

Fig. 1. A typology of scammers by size.

fraudsters also illustrate how they often work in networks for fees and percentages, but ultimately alone. In one case reported in the media in Ghana featured an interview with "Kofi", who made a modest living of €1000 per month buying stolen credit card information from Russian hackers which he then used to buy goods like laptops in the victims' countries and then using a network of associates for fees gets those items picked up and shipped to Ghana, where they are then sold (Youtube, 2020). Some lone fraudsters are very successful, making significant sums of money. In one interview with an active romance fraudster based in Ghana (Sakawa Boy), the culprit revealed he had dozens of victims on the go at any one time, requiring spreadsheets to manage them all and in one of his most successful enterprises, had made US$500,000 from a victim. He also used networks of others to help create profiles, do the initial recruitment and launder the money for which fees were paid (BBC World Service, 2023).

4.2. Gorgons

Gorgon is a creature in Greek mythology with three heads whose appearance turns the beholder into stone. Gorgons seems appropriate to, therefore name couples and small groups under 10. There are many examples of couples and small groups of scammers which can be found that fall into the 'Gorgons' category of <10 who engage in fraud. An academic interviewed with expertise on Ghana scammers noted:

> They are small. Often what I heard is that they are small groups of friends, like people who know each other and then, and who … sometimes who work together, who sometimes they have some kind of division of labour that some people are better at kind of getting people in, some people are better at kind of getting something out of people at certain like phases of the scam, that if you are kind of done with somebody like if he has kind of seen through the scam, you give him to somebody else, and also, like I often heard, there's a lot of that people also like that … like a very loose network of people who have technical expertise. Who? (Academic 2).

Searches of cases also revealed this size of enterprise to be common in many countries. In 2024, a couple based in the UK were convicted of perpetrating romance frauds against Australian and US citizens, among others, and then moving monies to Ghana. The fraud amounted to several hundreds of thousands of pounds (National Crime Agency, 2024). There are often very small groups that work together but are not couples. For example, in Nigeria, Bamgboye Adewunmi was convicted in 2023 for his role with two others in attempted business email compromise frauds against US companies worth almost US$1 million (The Nation, 2023). In another case where the fraudsters only operated domestically, three men in 2020 were convicted of running a boiler room in London and selling worthless investments in diamonds from an office in London (City of London Police, 2020). A tactic used by some fraudsters is to go to a third country to target their home country with the belief that local law enforcement will be less interested because there are no victims in their country. In one such case from the Far East in 2022, a gang of five South Koreans were arrested in Thailand after previously being based in China, where they had targeted their home country with telephone scams (The Nation, 2022).

4.3. Ogres

Ogres are mythical giant creatures that eat people. Ogre is appropriate to link to the next category of groups of bad actors working together of less than 50, but more than 10. This size of enterprise can be commonly found in West Africa, India and South East Asia. A fraud consultant in Ghana illustrated some of the more organised enterprises in his country, and Nigeria fitted this category:

> hardcore organized crime is different. So, for instance, for the Nigerians we have arrested in Ghana. You go there. You see them in the room. You can see about 30 individuals in a single room, and when you [unclear] into the room you see them with over 50 laptops. (Ghana Fraud Specialist).

In another case from India a centre was raided exposing a bogus company called Avenir Pvt Ltd, which was allegedly targeting American citizens with telephone scams. The ring leaders, Rajesh Khan alias Rajesh Mukherjee and his recruiting officer Naomi Changsan were arrested, equipment seized, and 36 employees were also picked up by the police (The Telegraph, 2024). In Nigeria, scholars have called a recent development 'Hustle Kingdoms', which are illegal training schools for online fraudsters (Lazarus, Soares and Button, 2025; Lazarus and Soares, 2025). As an example, in 2024, Ikemesit Edet was convicted of running such a school with 10 trainees (Economic and Financial Crimes Commission, 2024; Lazarus, Soares and Button, 2025).

4.4. Behemoths and Mega Behemoths

Behemoth is a mythical large monster creature from the bible that causes chaos and is appropriate to describe larger enterprises. The numbers that fit this category of between 50 and 250 and 250+ for the Mega Behemoths in the illicit world of scamming and organised crime are hard to distinguish accurately, although evidence will shortly be provided of some very large enterprises. The challenges, however, make it best to consider these two categories together. There have been a number of exposures of groupings of this size in Nigeria, Ghana, India and South East Asia. Some of these examples will now be explored.

By their very nature organised crime groups are secretive and obviously do not publish their 'staff numbers' and turnover. However, there are a number of organisations which have been linked to fraud of which there is evidence of their significant size through indictments, prosecutions and by the media. A study of Nigerian romance fraudsters that many groups comprised, "syndicates of 150–200 scammers" overseen by "Chairmen" operating at three levels (Andoh-Baidoo et al., 2024, p 124). There have been many exposures in India of enterprises of this size. In one case of a call centre operation based in India targeting the USA with fake IRS and

immigration service calls, it was suggested to have generated $300 million, the US indictment of the gang noted 24 key persons in the US (involved in the money laundering), 32 key leaders in India, but with subsequent media reports suggesting 630 staff working in the call centre and 197 arrested on a raid (CNN Money, 2017; Hindustan Times, 2018; Times of India, 2018). Two fraudsters from India interviewed for this research also confirmed the size of these operations:

> The size of the call centre ranges right from 10 people to 150/200 persons (India Fraudster 1).
>
> There were floors and floors of young boys and girls 100s in number doing the IRS (Internal Revenue Service scam). The salary and incentive were crazy. Youngsters had a competition amongst them to do this (India Fraudster 2).

The other area where there are large organisations are the 'forced labour' scam centres/compounds of South East Asia. There is evidence of significant entities linked to organised crime involved in these compounds, with a UN report estimating they generate billions of dollars and in Myanmar, there could be 120,000 held in scam compounds and 100,000 in Cambodia (United Nations, 2023). The scale of one operation can be illustrated by the US Department of the Treasury indictment against the Prince Group, who were alleged to be running scam compounds in Cambodia, which amounted to $15 billion of seized assets in bitcoin from these activities (US Department of the Treasury, 2025; United States Department of Justice, 2025). The scale of this and other compounds clearly suggests enterprises of Behemoth level plus. Further evidence of the size is illustrated by one raid on a scam compound centre in the Philippines freed 1100 persons, who it is alleged were forced to conduct cryptocurrency scams (Franceschini et al., 2023; 2025). Some of the compounds operating in this region are large, "… purpose-built for online operations, and include offices, dormitories, and space for shops, entertainment, and other amenities" and a "single compound is usually overseen by a property manager and contains several scam companies, often along with shared canteens, brothels, clubhouses, clinics, pharmacies, and services of all sorts, ranging from restaurants to hair salons (Franceschini et al., 2023; 2025, p 579). The size of these entities has meant traditional company structures have emerged such as managers, human resources departments and security to maintain discipline and stop escapes. In one real case from Myanmar, Franceschini et al. (2023, p 586) found one call centre with 294 staff. The evidence from raids, size of compounds and broader macro data lead us to the conclusion that there are highly likely to be *Mega Behemoth* sized operations in this region engaged in scamming.

The Nigerian confraternities such as Black Axe have been linked to perpetrating frauds such as Business Email Compromise (BEC) and money laundering, along with many other criminal activities (Button et al., 2025; Lazarus, 2024). These confraternities are secret cults that emanate from Nigerian universities and in Nigeria. Ariyo (2021) has estimated that in the 50+ universities in the Southern part of Nigeria, there could be 30,000 members in each university at any one time. Ariyo (2021) noted the scale: "As cult or confraternity membership is permanent and for life, then it is possible that there are close to tens of millions of members of these confraternities in different sectors across Nigeria and other countries, including Europe." This extensive network highlights these groups' pervasive influence and reach, both domestically and internationally. Black Axe alone has been closely linked to the Neo-Black Movement (which it denies) and is estimated to have 3 million members globally (BBC News, 2021). In one case in Ireland, the size of the operation was illustrated by the successful investigation of one case linked to a sub-zone of Black Axe in Ireland, which involved potentially over 4000 in romance and business invoice fraud, combined with the money laundering of the proceeds. The investigators noted 838 Money mules (recruited living in Ireland) but believe there could be up to 4000 of these: 63 Herders (organising the mules); 50 Operational directors, and 16 Strategists at the top of the network (Irish Examiner, 2022). Interviews from the research also illustrated this too:

> But when you start looking at BEC fraud, when you look at the romance scam, so when you look at the investment scams. Those are all confraternity members that are conducting it. And I can state that with evidence that we've seized electronic evidence that we seized analysis that I've done personally myself as well in tandem with other countries (Law Enforcement South Africa).

5. Specialisation and a supporting cast of roles

The larger the groups involved the greater the specialisation in roles. There are, for example, those who specialise in finding victims, making initial contact and those who close the deal. This section will illustrate some of that specialisation. It is also important to note the scam ecosystem, like any industry, contains an extensive range of supporting 'sectors' and roles. Money laundering is an obvious one, but there are many others, such as website developers. Third, there are legitimate roles that often have to be corrupted to enable the schemes to continue to work seamlessly, such as the police, politicians and bankers, to name some. These different specialisms and roles will now be considered.

5.1. Specialisation within scam enterprises

Past research on telemarketing fraud in the USA has illustrated specialisation in call centres between frontline 'sales' staff, 'closers' who are better sales agents and 'reloaders' who are the most effective sales agents, overseen by managers and owners (Shover et al., 2004). A natural consequence of a growing sector and entities within it is specialisation. While we provide four examples of scam enterprises from the larger end of the scale of enterprises (Ogres, Behemoths and Mega Behemoths) to illustrate the degree of specialisation that exists in the scamming ecosystem, we draw on our public-facing research from this project (Button et al., 2024) and other published papers (e.g., Franceschini et al., 2023; 2024; Lazarus, Chiang and Button, 2025; Wang and Topalli, 2024a).

Scam centres operate with a high degree of specialisation, resembling legitimate enterprises with distinct roles dedicated to

different aspects of their operations. Wang and Topalli (2024a) have noted the specialist recruitment and roles "chat moderators" or "customer service providers" to conduct operations to generate leads for others in the operation to then scam. The Indian scam centre model is structured with data sellers, openers, senior closers, human resources, trainers, managers, and owners, while money mules and hawala networks handle financial transactions (Button et al., 2024). Similarly, the Southeast Asia scam compound model is hierarchical, with a head overseeing operations, managers supervising team leaders, and scammers divided between "heavenly scams" (gambling fraud) and "earthly scams" (investment or pig butchering fraud) (Lazarus et al., 2026). Supporting roles include human resources for recruitment, logistics teams ensuring operational infrastructure, security staff, and auxiliary services such as canteen workers and personal service providers (Lazarus et al., 2026). In the West African "Hustle Kingdom" scam centres, roles include trainees, profilers who identify victims, closers skilled in manipulation, and an overall leader, or *Oga,* according to empirical research (Lazarus, Soares and Button, 2025). Money laundering is managed by herders and mules, in such organised illicit groups (Button et al., 2025). The Nigerian Confraternity, such as Black Axe, follows a structured hierarchy (Cohen, 2023). with a national leadership council, zonal heads, a chief priest responsible for spiritual ceremonies, a butcher enforcing discipline, a treasurer (*Ihaze*), a communicator (*Cryer*), and axemen performing various scam-related tasks similar to the West African model. Across these scam enterprises, specialisation is key to ensuring efficiency in victim exploitation and financial operations. (Sources: Interviews, Cohen, 2021; Cohen, 2023; Franceschini et al., 2023; 2025; Lazarus, Soares and Button, 2025; Soares et al., 2025).

A scamfighter who knew the business of West African scammers very well illustrated how some specialise in finding victims, while others more skilled in sales/manipulation closed the deals:

> … the people that facilitate the fraud, the people that and engage with reach out to victims, engage with the victims and once they get enabled a bite, they'll actually give it through to the more professional part of the syndicate to actually engage with the victim … get the victim to do things by money, etc. That's what it's all about. And then we've got, of course, the Oga sitting at the top of the group, very informal (Scamfighter 1a).

The specialism of these centres and ability to run multiple targeted and successful scams was illustrated by one scamfighter monitoring one group:

> and this group is so extensive that they developed right now, and they are still going. I struggle to keep the steps with them because they have 600 sites at once. When you go after them. They develop specific type of scams for specific geographic areas. So they have a bunch of fake sites that are targeting entirely Europe with investment scams with next of kin scams, with loan scans. Then you have another bunch of sites that are targeting Middle Eastern Asia with job scams, employment scams and such. Then you have another bunch of sites targeting U.S.A. with procurement scams, and you have a 4 level of sites, fake sites that are targeting Africa small businesses willing to develop and grow. And they are using the same email addresses used to scam before (Scamfighter 1b).

Some of the West African scammers have built global networks to facilitate money laundering. A senior law enforcement official commenting on Ghana's organised groups (many of which are run by Nigerians who may be linked to confraternities) noted:

> What sets them apart is their global reach, as they have members located in various countries outside Ghana, predominantly in Europe, Canada, and the USA. This international network allows them to seamlessly launder money and engage in other criminal activities to further their fraudulent endeavours. Through this intricate chain, they can pool resources and carry out their illicit activities with greater efficacy (Ghana Senior Law Enforcement).

Indian call centres can also be relatively simple, but some of the larger enterprises have human resource departments, trainers etc. Some of the centres in India also merge into legitimate businesses, indeed some call centres do both legitimate and illegal calls, as one government official noted:

> … they are, sort of, multi-functional and hybrid roles, so some of them might be operating generally, genuinely … you know, a genuine call centre in the daytime or whatever, and then using that process … and then using it as an illicit call centre at night, a scam centre at night (Government official 1).

The merger and blurring of scam centres with legitimate businesses was also noted by one scamfighter interviewed:

> [name of scam owner] and his associates own things like night clubs. They were running their own scam call centers as well. But there was something called [name] nightclub in Delhi, where again it was looked like a completely legitimate, legitimate business alongside the scamming one. And that's what you tended to find …. (Scamfighter 2).

These scam centres are relatively simple, however, compared to the South East Asian scam compounds and Nigerian confraternities. In Southeast Asia, Franceschini et al. (2023; 2025) and Lazarus et al., (2026) have found evidence of large enterprises with very sophisticated structures with managers, team leaders, human resource departments, logistics as well as a variety of specialist services from hair salons, pharmacies and brothels located on site to support the centres. In west Africa, the Nigerian confraternities, such as Black Axe, also have sophisticated organisational structures broken into zones with a chairman in charge and a variety of other specialized roles (Button et al., 2025; Cohen, 2023). Increasing size brings greater specialisation and in all probability greater effectiveness.

5.2. Supporting industries

There is also a supporting industry of roles that the scam ecosystem requires to operate effectively. Some call these 'enablers' play a very important role such as producing websites and ensuring they are rejuvenated as quickly as possible after a takedown (Lazarus and Whittaker, 2025; Whittaker, 2024; Whittaker et al., 2025). The specialist help scammers turn to also varied depending upon the location as one interviewee noted:

> now, typically what we will see, though with the Nigerians is they keep their scams very much in house the extended family people from the region, or people that can trust with the Cameroonians, … will actually involve the local populace in these scams … as the Nigerian side, will run it like family business, basically keeping it in the family (Scamfighter 1a).

Some of the different areas of specialisation will now be considered.

i) Website development and hosting

Many scams are built upon fake websites, which need to be built (Whittaker, 2024; Whittaker et al., 2025). AI maybe making it easier to do this, but many fraudsters turn to specialized web-developers to do this work. As noted above Nigerians tend to turn to specialists from extended family, region, where as other bad actors can be more global in the sourcing of these specialist IT services, such as Cameroonians using specialists from the Indian sub-continent. Some of these specialists work solely in developing fake websites, others have a mix of trade and turn a blind eye to the fraudulent. A scamfighter specialising in this area taking down websites noted:

> What they will do is they will actually get somebody that's quite professional. I won't say professional. But that can put up a good looking website. Yeah, the thing is what you will see is like, I said, there's a lot of different types of websites that we have together in these camps where as advance free fraud, where you sell something that doesn't exist … (Scamfighter 1a).

He went on to note they even create fake bank websites to convince victims they have money:

> It looks like a client area, and it can transfer money, but it seems he wants to transfer this money there. All these fictitious costs, and so built into the template. Some of these templates are quite sophisticated with initially, we saw it was just basically a little Javascript to put that way. So it looks like there is a bank account there. It's actually become quite sophisticated now … (Scamfighter 1a).

Some of the other areas where fake websites are built include: banks, couriers, fake lawyers. Romance websites, gaming, crypto currencies to name some. Building a website is only part of the challenge as they also need to be hosted and redeployed as soon as they are taken down and there are those specialising in this too who are very quick at redeploying sites:

> …. the importance of the fraud facilitator. We had sites that were reported to the hosting provider because the registrar said that content is not a registrar issue, right. It's a hosting issue and a fake lawyer site, for example, jumped 27 times from a host to another host (Scamfighter 1b).

Some of those servicing the industry even offer one stop shops providing all the services necessary:

> They will actually sell you the templates. Everything that you need is a one-stop shop and what you will find is they will have multiple syndicates that they're feeding at the same time (Scamfighter 1a).

ii) Document production

Many of these bad actors specialising in websites also offer other services such as the production of fake documents which have become increasingly sophisticated and hard to detect (Baechler, 2020). Documents proving bank accounts, ownership of land assets, invoices etc are also frequently used in scams. Just like the websites there are also bad actors specialising in the production of these documents.

iii) Social media influencers

Social media has become a significant vector in promoting scams and several social media influencers have become implicated in a number of high-profile scams (McNealy, 2022; Qureshi et al., 2024; Shepherd et al., 2023). The Nigerian social media influencer, Ramon Abbas, AKA Hushpuppi, who flaunted a lifestyle of riches was found to have been implicated in millions of dollars worth of money laundering resulting from scams was jailed in the US (Sky News, 2022). In another famous case from Ghana, Mona Faiz Montrage, another social media influencer was jailed for her part in money laundering proceeds from a variety of scams, particularly romance (United States Attorney's Office, 2024). These prominent cases illustrate the roles of influencers in money laundering, but many also promote scams knowingly, some are tricked into doing so and in some cases their accounts are hacked or are fake (Marzouk, 2023). A cyber security expert from Ghana noted:

> … fraudsters impersonate prominent people in society including members of parliament, ministers, clergy among others on social media and use the profiles to promote investment opportunities like ponzi schemes with very high returns (Ghana Cyber Security Expert).

The challenges of identifying who is behind a social media account makes identifying the culprit difficult. The evidence suggests, nevertheless, there are specialists in social media who develop fake profiles, impersonate or hack others' accounts, trick real users into promoting or simply use their own to share posts that are either directly scams or lead someone to be lured into act which puts them at risk of a scam.

iv) Spiritual strategies in online fraud

Spiritual support for scamming is very important among some scammers in West Africa and the priests who provide this support secure fees from the scammers (Akanle and Shadare, 2019; Alhassan and Ridwan, 2023; Aransiola and Asindemade, 2011; Lazarus, 2019; Lazarus and Okolorie, 2019; Monsurat, 2020). The priests supplying these services have therefore become an important part of the ecosystem in West Africa. The importance of this will be briefly illustrated. The use of Juju is central to some scammers in their beliefs; it – in their minds - will make them successful in enticing victims to part with their money (Alhassan and Ridwan, 2023; Akanle and Shadare, 2019; Lazarus, 2019; Oduro Frimpong, 2014; Tade, 2013). This involves perpetrators incorporating supernatural beliefs or rituals to enhance their illicit schemes. For instance, some scammers reportedly employ hypnotism to manipulate their victims (Lazarus, 2019; Tade, 2013), while others seek assistance from priests or spiritual practitioners who provide charms or amulets intended to increase the effectiveness of their scams (Akanle and Shadare, 2019; Lazarus and Okolorie, 2019). These spiritual strategies form part of a broader array of rituals utilized to augment the perceived success rate of fraudulent activities.

Online scammers' integration of spiritual tactics has been documented in various parts of West Africa, notably empirical studies in Ghana (e.g., Alhassan and Ridwan, 2023; Yushawu and Jaishankar, 2025), Nigeria (e.g., Lazarus and Okolorie, 2019; Monsurat, 2020), and Cameroon (Whittaker et al., 2025). In these regions, some individuals believe supernatural methods bolster their fraudulent endeavours (e.g., Monsurat, 2020). Cybercriminals argue that integrating spiritual practices not only aids in achieving their goals but also provides protection against law enforcement detection (Lazarus and Okolorie, 2019; Monsurat, 2020; Yushawu and Jaishankar, 2025). Our data analysis supports findings from Ghana and Nigeria, confirming the regional belief in the efficacy of these practices. According to several participants, this involvement was noted, and how it works:

> Its crazy, all kinds of sacrifices and fetishes for those not making enough money (Scamfighter 5).

Scammers require some personal item of the victim such as a photo or item of clothing,

> (regarding a romance fraud victim who sent a photo to the scammer) the photo was probably more suitable to whatever ritual he subscribed to. But what it also does as well, which I found really interesting, is how confident it makes them. You know, the actual criminal, when they've done the ritual, they really believe that they've got a hold and power (Consultant).

Once the ceremony has been completed, one ex-Yahoo boy noted:

> Now whenever a client has been looked, anything you ask him he should provide for you. So, that's it. And sometimes [inaudible 00:22:17] anything you tell, he do (Yahoo Boy 4).

In Anglophone[1] West Africa, internet scammers in Ghana, known as "Sakawa Boys" (Alhassan and Ridwan, 2023; Lazarus et al., 2025; Oduro-Frimpong, 2014; Yushawu and Jaishankar, 2025), and those in Nigeria, referred to as "Yahoo Boys" (Akanle and Shadare, 2019; Lazarus and Okolorie, 2019; Monsurat, 2020), are reported to sometimes blend spiritual beliefs with conventional scam techniques to manipulate victims globally. This fusion of spiritualism and fraud represents a specialized role within the larger scamming ecosystem, illustrating the adaptive strategies employed by criminal actors to enhance their success rates. Interestingly, blending supernatural strategies into online fraud has rarely been reported among scammer groups outside African diaspora communities, suggesting a possible form of exceptionalism in this context, according to a systematic review of empirical literature from 2000 to 2021 (Lazarus et al., 2023). Understanding these practices offers insights into the justifications, worldviews, and ideologies of those who perpetrate scams. It also highlights the cultural nuances within West African societies that shape various forms of online fraud globally. Despite often being overlooked or dismissed by popular cultures, particularly in the West, spiritual and magical beliefs continue to evolve within modern African diasporic societies (Bever and Styers, 2018; Lazarus, 2019). As such, advancing our understanding of the spiritual aspects of online fraud is crucial, yet this dimension remains under-theorized. We thus consider the role of spiritual strategies in online fraud, aiming to contribute to a more comprehensive understanding of the global scamming ecosystem and the specialized roles that have emerged within it.

[1] While some of these instances may be evident in other non-English-speaking regions of Africa, we acknowledge that the authors of this study are not proficient in other dominant publication languages, such as Portuguese. This barrier may have shaped our access to relevant literature in on-English publications; therefore, our discussion pertains primarily to English-language sources.

5.3. Corrupt and indifferent actors

Corruption also underpins the scamming ecosystem at a number of levels in different countries. At the most extreme, particularly in South East Asia, scammers operate under the local 'protective umbrella' of political and economic elites that actively profit from scam operations established by (mostly ethnic Chinese) outsiders (Franceschini et al., 2023; 2024; 2025; Lazarus et al., 2026; Loughlin, 2024). At another level there are actors such as government officials, law enforcement, bankers to name some who for bribes either facilitate scamming or turn a blind eye to such activities. Some of these actors are openly corrupt and work for scammers, some simply do not ask questions and others are just incompetent or disinterested. Such corruption has varied causes, not all endogenous (Hall and Yarwood, 2024).

The interviews for this research project and other sources have identified in many countries where scammers operate there are often corrupt law enforcement. These officers provide a variety of services for a fee, from tipping off scammers they are about to be raided, to turning a blind eye to their operations to letting them go when they are arrested. One scammer in Ghana interviewed claimed to have bribed a police officer to be released when they had been arrested and a Nigerian fraudster interviewed argued it was more in the interests of the police to be paid off than to arrest. Another Ghana expert noted:

> … sometimes we know that this particular house comes to a lot of suspected fraudsters ….So sometimes the police will choose to go there and then they pay them, and then they go (Ghana Security expert).

One scamfighter interviewed argued it was endemic in Nigeria, but the reach of corruption was global too, including even the USA:

> Nigerian groups like Black Axe they've bought into the court system. They have judges on their payrolls. They have law enforcement on their payroll. So the group we work with our vetted folks globally. We wouldn't work with any local law enforcement because of the trust issues. And we've seen this. I mean, I'm not just talking South Africa if they own judges in America, politicians in America, law enforcement, etc. And we can see it when we arrest them and we go to court (Scamfighter 3).

Even if scammers are jailed there has been some evidence to illustrate going to prison is no barrier to continuing scamming. In one case from Nigeria, a scammer serving a 24 year prison sentence was implicated in conducting a $1million scam while in jail, with suggestions corrupt officials there enabled him to carry on (BBC News, 2019). Politicians and government officials are also key players in helping some scammers operate. Many Nigerians liken Yahoo Boys to politicians (“Yahoo Men”), given shared associations with corruption and bribery (Lazarus, Button and Adogame, 2022). Similar comparisons extend to religious leaders, labeled "Yahoo Men of God" (Lazarus, Tickner and Button, 2025). Such comparisons signal a legitimacy crisis in which fraud is normalised as another form of elite extraction, weakening moral boundaries and public trust.

Beyond this symbolic legitimacy, scammers also draw on mundane commercial infrastructures, adopting standard business tools to widen their reach and credibility. Some scammers use normal business marketing tools and strategies too. They purchase them like any ordinary business would. As was noted by one expert:

> Cameroonian style scales, because Cameroonian is fake e-commerce. Basically they will actually use normal marketing tactics against consumers. They will use SEO advertising everything. And typically you're gonna find that in the Indian Bangladeshi Pakistani space (Scamfighter 1b).

Indeed, many social media companies have been criticised for inappropriate vetting of adverts, leading to many scams scoring high on search engines (Guardian, 2023). Further a recent leaked Meta document suggested they earn 10 % of their revenues from scams earning about $7 billion a year (Reuters, 2025). Such significant amounts create conflicts in effectively tackling the problem and so for many tech providers corruption might not be an issue, but conflicts of interest may lead to a lack of scrutiny and concerted action.

In Nigeria, universities are important in the facilitation of fraud (Aransiola and Asindemade, 2011; Lazarus and Okolorie, 2019). There is no evidence that universities direct fraud, but there is the use of their infrastructure to recruit students into corrupt endeavours, most notably the work of confraternities such as Black Axe. There is also evidence that some universities have very high degrees of penetration of active fraudsters. With two Nigerian law enforcement officials noting in some areas:

> But I can tell you categorically that if you get 100 undergraduates now and you sample them statistically, I can categorically tell you that 80 per cent, 80 over 100 male undergraduate students are into cybercrime (Nigerian Law Enforcement 3).

> many undergraduates are mostly involved because you find it's unless you for you to find eight or nine out of 10 graduates in any town where there is a higher institution which is southwestern (Nigerian Law Enforcement 2).

With such high rates of penetration in some areas, at best the universities could be described as incompetent or at worst complicit in such widespread bad acts and although a small body of evidence there was some of staff involvement at universities in Nigeria, with one scamfighter noting a scammer they identified:

> … was a lecturer (by) day, and he was doing cryptoscams and if you actually have a look at the end of the day, yes, some of the people that come from the same university down in the South East … also involved in cryptoscam (Scamfighter 1a).

Legitimate recruitment agencies have been previously noted in recruiting persons into jobs that turn out to be scamming (Lazarus et al., 2026; Wang and Topalli, 2024a). This research found recruitment agencies were used in India to recruit call centre workers. Some of the workers are recruited to what they think is a legitimate operation, but as soon as they start to realise it's not, and either

leave or embrace it. Some recruitment is also clearly orientated to criminal activities from the start. However, one scamfighter working in this area noted how legitimate recruitment agencies were used.

> But there, I saw the system as more organized. They had short training done for the new recruits. Recruitment of new people was mostly facilitated from recruitment agencies, and they are given mandates to send biodata of young boys and girls who speak English to outbound call centers (India Fraudster 2).

Insiders who provide information on potential victims, security procedures and who circumvent established procedures are also important in facilitating frauds. One Indian fraudster interviewed alluded to corrupt insiders providing lists of potential victims and even using their existing skills in developing legitimate scripts in call centres to create scam scripts.

> Entire script is received from the USA or the home country, wheresoever we are calling. Our target predominantly is the USA. This type of fraud is not possible without deep involvement in the home country. How are we supposed to get the call list, the list of vulnerable person, the mule accounts without involvement of local agencies (DP Fraudster X).

Insiders, particularly in banks, are also very important for money laundering. An Irish law enforcement officer also illustrated how the scammers cultivated insiders in key positions in Western countries too:

> … we've arrested [those involved in scamming] working in banks, working in social media companies working in accountants working in places where they have access to data now and what they're doing with the data, whether they're seeing the data or whether they're just learning the tricks of the trade …

He went on,

> We had a bank, a bank employee actually calling out to people's houses, collecting the cards (bank) from people (mules) you know … (Irish Law Enforcement Officer).

6. Evolutionary fraud or scamvolution

Evolution describes a process where, by natural selection, the fittest and most effective organisms survive and prosper, resulting in a diversity of beings suited to their environment (Gregory, 2009; Laszlo, 2009). The process of evolution is not restricted to the natural world. Evolution can also be seen in economics (Beinhocker, 2007; Herrmann-Pillath, 2013), where the most adaptable and resilient businesses survive amid fierce market competition.

The emergence of a substantial scam ecosystem has unleashed forces of evolution operating at two levels. First, the vast number of different types of scams that emerge on a day-to-day basis because of the natural evolutionary process more successful scams emerge. Poor scams fail and disappear, scams that succeed are refined and replicated. Second, the lack of global enforcement to disrupt and destroy scamming enterprises means that successful entrepreneurs thrive and grow and are copied; those that fail disappear. The evolutionary process by natural selection is breeding ever more effective scams and, most alarmingly, stronger and more efficient entities to deliver these scams. The sheer size of bad actors and their activities in the scamming ecosystem are driving innovation, specialisation, and even greater success from scammers.

6.1. Innovation

Law enforcement generally does not have much impact on these bad actors – very few are apprehended. The biggest challenge is not law enforcement catching them it is the activities of largely private actors who, by various innovations, move to better protect their organisations and customers. Data analytics, often linked to AI – for example is increasingly used by the banking world to detect fraudulent transactions and prevent them from occurring (Kim et al., 2019). That makes certain credit card frauds more difficult, driving them to innovate to find new means of attack. So many romance fraudsters who previously used photographs of real people, which can be detected through an image search, now use AI to create images. Many fraudsters are now using a variety of AI technologies to perpetrate fraud innovating to be more successful.

6.2. Specialisation

Much of the discussion above has illustrated the increasing specialisation of roles in scamming from a variety of roles in scamming enterprises through to the wide range of facilitators and corrupt actors. Just like evolution has driven numerous specialized creatures and plants to adapt to their particular environments, this is occurring in scamming.

6.3. Spreading and replications

The production of multiple scams and scammers has also fuelled their spreading and replication, as some actors move abroad or others simply observe what is happening elsewhere and replicate with refinements (Lazarus et al., 2025). Some of the experts interviewed noted this process:

> The problem is, when they are moving abroad, they are taking their scams with them, and they are keeping them doing it … They are going to businesses abroad, and they are going with the scams with them, and they are developing their scams and everything. So you have (Scamfighter 1b).

> So what seems to happen, in my opinion, or my observations over the last 40 years, is that some of the people that they recruit will then go off and do it on their own as well. So people will work with the organised gangs to learn how to do it, but then they'll also go off and do it themselves. And then they'll teach their friends. Or what happens with that, is they become less efficient, so they don't have the same degree of operational security (Counter Fraud Consultant UK).

7. Fraudsters outnumber and out-resource law enforcement

The substantial size and resources of the scammers also poses a significant challenge to law enforcement. The size of some operations dwarfs the capacity of many economic crime units investigating such frauds and the totality of law enforcement in some countries. For example, in England and Wales it was estimated there were 1753 officers and staff in 2021 dedicated to economic crime spread across multiple agencies (Hyde et al., 2022). As was noted earlier there is evidence to suggest some organised groups in fraud have a larger staff count and access to substantial resources.

The in-balance in resources has substantial implications. Fraudsters have greater resources to protect and improve their 'business'. They can invest in the latest technologies, bribe key persons to protect their enterprises, hire the best lawyers to repel legal proceedings and purchase security to protect themselves. Resources also enable them to move when the going gets tough in a particular location. There is already evidence of Nigerians moving to Ghana where operations are smoother (Lazarus et al., 2025).

8. Discussion and conclusion

This study has examined the scamming ecosystem developing a novel classification rooted in size and structure, categorizing fraudsters based on organizational structure into operations of varying in size and complexity.

- Demons (Sole Traders): Independent actors making swift decisions with minimal risk of betrayal. Despite limited resources, they can exploit multiple victims.
- Gorgons (Micro Enterprises): Small groups leveraging shared skills, increasing efficiency. Trust is crucial, often forming among friends or couples.
- Ogres (Small & Medium Enterprises): Larger groups enable specialisation, expanding operations with structured roles.
- Behemoths & Mega Behemoths (Large Enterprises): Resembling corporations, they operate scam call centres and international networks, showcasing sophisticated fraud structures.

The study has also introduced the novel concept of "scamvolution," likening scam evolution to natural selection, where successful scams adapt and persist through.

- Adaptation to Law Enforcement and the anti-scam community: Scammers refine techniques, such as shifting to AI-generated fraud.
- Imitation of Legitimate Businesses: Larger scam operations mimic corporate structures for efficiency.
- Spatial Embeddedness: Certain regions serve as cybercrime hubs due to socio-economic and cultural conditions.

Prior research (Button et al., 2025; Shover et al., 2004) contextualises this within broader cybercrime trends, while the role of cyber spiritualism in West African scams (Aransiola and Asindemade, 2011; Alhassan and Ridwan, 2023; Lazarus and Okolorie, 2019) highlights underexplored cultural influences.

This paper aids the anti-scam community and law enforcement by providing a deeper understanding of scam structures through.

- Targeted Law Enforcement and anti-scam community action: Larger networks require international cooperation of state and private actors.
- Regulatory Policies: Industries enabling scams (e.g., web hosting, social media) need stricter oversight.
- Capacity Building: Investing in technology and training enhances scam detection.

Corruption exacerbates these issues, as insiders may facilitate fraud, eroding institutional trust and complicating international cooperation. Spiritual practices in cybercrime, particularly in West Africa, reinforce scammers' confidence and legitimacy within their networks (Lazarus, 2019; Lazarus and Okolorie, 2019; Monsurat, 2020; Yushawu and Jaishankar, 2025). This reflects a unique cultural element in fraud tactics, warranting further study. By analyzing scam operations through organizational and cultural lenses, this study deepens our understanding of their adaptability, impact, and necessary countermeasures.

CRediT authorship contribution statement

Mark Button: Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization. **Suleman Lazarus:** Writing – review & editing, Writing – original draft, Project

administration, Methodology, Investigation. **Branislav Hock:** Writing – review & editing, Methodology, Investigation, Conceptualization. **Paul Gilmour:** Writing – review & editing, Methodology. **Durgesh Pandey:** Writing – review & editing, Methodology, Investigation. **James Bugbilla Sabia:** Writing – review & editing, Methodology, Investigation.

Funding

This project was funded via ITAD from the UK Government Home Office.

Declaration of competing interest

The authors declared no conflicts of interest.

References

Akanle, O., Shadare, B.R., 2019. Yahoo-plus in ibadan: meaning, characterization and strategies. International Journal of Cyber Criminology 13 (2).
Alhassan, A.R.K., Ridwan, A., 2023. Identity expression—the case of 'Sakawa' boys in Ghana. Human Arenas 6 (2), 242–263. https://doi.org/10.1007/s42087-021-00227-w.
Andoh-Baidoo, F.K., Offei, M.O., Ayaburi, E.W., Siponen, M., Gladyshev, P., 2024. How do real cybercrime syndicates operate?: the case of online romance fraud syndicates. IEEE Security & Privacy 22 (4), 124–128.
Aransiola, J.O., Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychol., Behav. Soc. Netw. 14 (2), 759–763.
Ariyo, D., 2021. Nigerian confraternities and the increase in human trafficking across Europe. Retrieved from. https://afruca.org/blog/nigerian-confraternities-and-the-increase-in-human-trafficking-across-europe.
Auwal, A.M., Lazarus, S., 2025. Experiences of local victims of Yahoo Boys' socio-economic cybercrimes in Nigeria. Discover Psychology. https://doi.org/10.1007/s44202-025-00479-5.
Baechler, S., 2020. Document fraud: will your identity be secure in the twenty-first century? Eur. J. Crim. Pol. Res. 26 (3), 379–398.
BBC News, 2019. Internet fraud: nigerian scammer 'pulls off $1m heist' from prison. https://www.bbc.co.uk/news/world-africa-50480495.
BBC News, 2021. The ultra-violent cult that became a global mafia. https://www.bbc.co.uk/news/world-africa-59614595.
BBC World Service, 2023. Sakawa boy reveals how scams work – love, Janessa. https://www.youtube.com/watch?v=NOq1SjLVYOQ.
Beals, M., DeLiema, M., Deevy, M., 2015. Framework for a taxonomy of fraud. Stanford: Stanford center on longevity. Available at: http://fraudresearchcenter.org/wp-content/uploads/2015/07/FFRC_Taxonomy_FullReport_7-22-15.pdf. (Accessed 21 October 2016).
Beek, J., 2020. Waiting, relationships and money in a Ponzi scheme in Northern Ghana. Critical African Studies 12 (1), 107–120. https://doi.org/10.1080/21681392.2019.1697315.
Beinhocker, E.D., 2007. The origin of wealth: Evolution, complexity, and the radical remaking. In: of economics. Random House Business Books, London.
Bever, E., Styers, R., 2018. Magic in the Modern World. Pennsylvania State University Press, Pennsylvania.
Button, M., Cross, C., 2017. Cyber Frauds, Scams and their Victims. Routledge.
Button, M., Lazarus, S., Hock, B., Bugbilla Sabia, J., Pandey, D., Gilmour, P., 2025. Factors influencing involvement in cyber-frauds in West Africa and the implications for policy. European Journal on Criminal Policy and Research 1-23. https://doi.org/10.1007/s10610-025-09649-6.
Button, M., Lazarus, S., Hock, B., Sabia, J., Gilmour, P., Pandey, D., 2025. Nigerian confraternities and mass cross-border fraud. Trends Organ. Crime 1–21.
Button, M., Lazarus, S., Hock, B., Sabia, J., Gilmour, P., Pandey, D., 2025. Nigerian confraternities and mass cross-border fraud. Trends in Organized Crime 1–30. https://doi.org/10.1007/s12117-025-09576-2.
City of London Police, 2020. Convicted fraudsters who offered worthless diamond investments ordered to pay back £172 987. https://www.cityoflondon.police.uk/news/city-of-london/news/2020/template3/convicted-fraudsters-who-offered-worthless-diamond-investments-ordered-to-pay-back-172987/.
CNN Money, 2017. Indian police arrest alleged ringleader of IRS scam. https://money.cnn.com/2017/04/09/news/tax-scam-india-arrest-ringleader/.
Cohen, C., 2023. The "Nigerian mafia" feedback loop: European police, global media and Nigerian civil society. Trends Organ Crim 26, 340–357. https://doi.org/10.1007/s12117-022-09471-0.
Cohen, C., 2021. Nigerian confraternities to conquer the world? Retrieved from. https://ora.ox.ac.uk/objects/uuid:3494415e-2726-4a82-be53-9095351208d4/download_file?safe_filename=Cohen_2021_Nigerian_confraternities_to.pdf&file_format=pdf&type_of_work=Journal+article.
Economic and Financial Crimes Commission, 2024. Internet fraud academy proprietor bags 10 years jail term. https://www.efcc.gov.ng/efcc/news-and-information/news-release/9995-internet-fraud-academy-proprietor-bags-10-years-jail-term.
Ferrante, D.J., Holt, T.J., 2025. Assessing Cyberattacks in Response to Police Actions in Physical Space. Deviant Behavior 46 (9), 1125–1138. https://doi.org/10.1080/01639625.2024.2429730.
Franceschini, I., 2024. Sihanoukville: rise and fall of a frontier city. Pulse 3 (1), 35–51.
Franceschini, I., Li, L., Bo, M., 2025. Scam – inside South East Asia's Cybercrime Compounds. Verso.
Franceschini, I., Li, L., Bo, M., 2023. Compound capitalism: a political economy of Southeast Asia's Online scam operations. Crit. Asian Stud. 55 (4), 575–603.
Franceschini, I., Li, L., Hu, Y., Bo, M., 2024. A new type of victim? Profiling survivors of modern slavery in the online scam industry in Southeast Asia. Trends Organ. Crime 1–23.
GASA, 2024. Global State of Scams Report 2024.
Gregory, T.R., 2009. Understanding Natural Selection: Essential Concepts and Common Misconceptions. Evo Edu Outreach 2, 156–175. https://doi.org/10.1007/s12052-009-0128-1.
Guardian, 2021. Judge-orders-internet-fraudster-to-sweep-court-premises-for-6-months. https://guardian.ng/news/nigeria/national/judge-orders-internet-fraudster-to-sweep-court-premises-for-6-months/.
Guardian, 2023. Meta slammed over scam ads on Facebook featuring Australian TV personalities. https://www.theguardian.com/technology/2023/mar/28/australian-tv-networks-criticise-meta-over-inadequate-response-time-to-damaging-scam-ads.
Hall, T., Yarwood, R., 2024. New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. Prog. Hum. Geogr. 48 (4), 437–457. https://doi.org/10.1177/03091325241246015.
Hall, T., Sanders, B., Bah, M., King, O., Wigley, E., 2021. Economic geographies of the illegal: the multiscalar production of cybercrime. Trends Organ. Crime 24, 282–307.
Hindustan Times, 2018. After 14 months, Thane call centre scam mastermind 'Shaggy' granted bail. https://www.hindustantimes.com/mumbai-news/after-14-months-thane-call-centre-scam-mastermind-shaggy-granted-bail/story-Hxlk98eT3KOhm5tuQe2b0K.html.
Hock, B., Button, M., 2023. Non-ideal victims or offenders? The curious case of pyramid scheme participants. Vict. Offenders 18 (7), 1311–1334.
Home Office, 2023. Fraud strategy: stopping scams protecting the public. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154660/Fraud_Strategy_2023.pdf.
Hyde, R., Gibson, J., 2024. It's a fraudster's world. https://www.smf.co.uk/wp-content/uploads/2024/09/Its-a-fraudsters-world-Sept-2024.pdf.

Hyde, R., Corfe, S., Anderson-Samways, B., 2022. Fraud is now Britain's dominant crime, but policing has failed to keep up. https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.
Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice 47, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002.
Irish Examiner (2022) https://www.irishexaminer.com/news/arid-40984004.html.
Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S.K., et al., 2019. Champion-challenger analysis for credit card fraud detection: hybrid ensemble and deep learning. Expert Syst. Appl. 128, 214–224.
Laszlo, A., 2009. The Nature of Evolution. World Futures 65 (3), 204–221. https://doi.org/10.1080/02604020802392112.
Lazarus, S., 2019. Where is the money? The intersectionality of the spirit world and the acquisition of wealth. Religions 10 (3), 146. https://doi.org/10.3390/rel10030146.
Lazarus, S., 2024. Cybercriminal networks and operational dynamics of Business Email Compromise (BEC) scammers: insights from the “Black Axe” confraternity. Deviant Behav. 1–25. https://doi.org/10.1080/01639625.2024.2352049.
Lazarus, S., Chiang, M., Button, M., 2025. Assessing Human Trafficking and Cybercrime Intersections Through Survivor Narratives. Deviant Behavior 1–18. https://doi.org/10.1080/01639625.2025.2470402.
Lazarus, S., Chiang, M., Dimitrova, R.S., Thu, T.T., Essien, E., 2026. What Do We Know About Human Trafficking and Scam Compounds in Southeast Asia (2020–2025)? A Qualitative Meta-Synthesis of Coercive Deviant Enterprises. Deviant Behavior 1–33. https://doi.org/10.1080/01639625.2025.2604138.
Lazarus, S., Hughes, M., Button, M., Garba, K.H., 2025. Fraud as Legitimate Retribution for Colonial Injustice: Neutralization Techniques in Interviews with Police and Online Romance Fraud Offenders. Deviant Behavior 1–22. https://doi.org/10.1080/01639625.2024.2446328.
Lazarus, S., Okolorie, G.U., 2019. The bifurcation of the Nigerian cybercriminals: narratives of the Economic and Financial Crimes Commission (EFCC) agents. Telematics Inf. 40, 14–26. https://doi.org/10.1016/j.tele.2019.04.009.
Lazarus, S., Soares, A.B., 2025. From business centres to Hustle Kingdoms: historical perspectives on innovative models of deviant education. Int. Ann. Criminol. https://doi.org/10.1017/cri.2025.1.
Lazarus, S., Soares, A.B., Button, M., 2025. Pathways, Pressure, and Profit: Adaptive Innovation and Strain in a Convicted Cybercrime Academy Called Hustle Kingdom. Deviant Behavior 1–25. https://doi.org/10.1080/01639625.2025.2551790.
Lazarus, S., Tickner, P., Button, M., 2025. Pulpit, power, and predation: “Yahoo Men of God,” prosperity theology, and the Twin Fraud Triangles. Critical Research on Religion 13 (3), 333–354. https://doi.org/10.1177/20503032251381309.
Lazarus, S., Whittaker, J.M., 2025. Fake online shops rely on tech skills: what drives Cameroon’s web developers to assist online fraudsters. The Conversation, retrieved. https://theconversation.com/fake-online-shops-rely-on-tech-skills-what-drives-cameroons-web-developers-to-assist-online-fraudsters-252429.
Lazarus, S., Whittaker, J.M., McGuire, M.R., Platt, L., 2023. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). Journal of Economic Criminology, 100013. https://doi.org/10.1016/j.jeconc.2023.100013.
Lazarus, S., Button, M., Adogame, A., 2022. Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals (“Yahoo Boys”) and Politicians (“Yahoo men”). Heliyon 8 (11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142.
Lazarus, S., Button, M., Garba, K.H., Soares, A.B., Hughes, M., 2025. Strategic business movements? The migration of online romance fraudsters from Nigeria to Ghana. Journal of Economic Criminology, 100128.
Levi, M., 2008. The Phantom Capitalists, Revised Edition. Ashgate, Aldershot.
Loughlin, N., 2024. Transnational crime meets embedded corruption in Cambodia. Global China Pulse 3 (1), 27–33.
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 Organ. Crime 1–24.
Lusthaus, J., Holt, T.J., Levi, M., Kleemans, E., Leukfeldt, E.R., 2025. The evolution of Nigerian cybercrime: two case studies of UK-based offender networks. Eur. J. Criminol., 14773708251329695
Mars, G., 2019. Cheats at Work: an Anthropology of Workplace Crime. Routledge.
Marzouk, O., 2023. How scammers are leveraging social media platforms to promote cryptocurrency fraud. https://blockchaingroup.io/how-scammers-are-leveraging-social-media-platforms-to-promote-cryptocurrency-fraud/.
McNealy, J.E., 2022. Platforms as phish farms: deceptive social engineering at scale. New Media Soc. 24 (7), 1677–1694.
Monsurat, I., 2020. African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the yahoo boys in Ilorin, Nigeria. International Journal of Cyber Criminology 14 (1), 300–315.
National Crime Agency, 2024. Couple sentenced for romance fraud and laundering criminal cash. https://www.nationalcrimeagency.gov.uk/news/couple-sentenced-for-romance-fraud-and-laundering-criminal-cash.
Oduro-Frimpong, J., 2014. Sakawa rituals and cyberfraud in Ghanaian popular video movies. Afr. Stud. Rev. 57 (2), 131–147. https://doi.org/10.1017/asr.2014.51.
Qureshi, M.A., Shahzadi, S., Hussain, T., 2024. Exploring the role of Influencers' Perceived Fraud Between Influencers' credibility and consumer purchase intentions. International Journal of Professional Business Review 9 (1), 1–20.
Reuters, 2025. Meta is earning a fortune on a deluge of fraudulent ads, documents show. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.
Shepherd, D., Whitman, K., Button, M., Wilson, J.M., 2023. The impact of deviant social media influencers and consumer characteristics on purchasing counterfeit goods. Deviant Behav. 44 (12), 1746–1760.
Shover, N., Coffey, G.S., Sanders, C.R., 2004. Dialing for dollars: opportunities, justifications, and telemarketing fraud. Qual. Sociol. 27, 59–75.
Sky News, 2022. Instagram influencer Hushpuppi, who tried to steal £100m from Premier League club, jailed in US. https://news.sky.com/story/instagram-influencer-hushpuppi-who-tried-to-steal-100m-from-premier-league-club-jailed-in-us-12741458.
Smirnova, O., Hyslip, T.S., Holt, T.J., 2025. Are Active Users the Most Central to Hacker Social Networks? A Comparative Analysis of Public and Private Online Network Structures Among Hackers. Deviant Behavior 46 (7), 877–893. https://doi.org/10.1080/01639625.2024.2373356.
Soares, A.B., Lazarus, S., Button, M., 2025. Love, Lies, and Larceny: One Hundred Convicted Case Files of Cybercriminals with Eighty Involving Online Romance Fraud. Deviant Behavior 1–24. https://doi.org/10.1080/01639625.2025.2482824.
Suwitho, S., Budi Riharjo, I., Ary Dewangga, D., 2023. The nexus between Ponzi scheme and multi-level marketing systems: Evidence in Indonesia. Cogent Social Sciences 9 (1). https://doi.org/10.1080/23311886.2023.2178540.
Tade, O., 2013. A spiritual dimension to cybercrime in Nigeria: the ‘yahoo plus’ phenomenon. Hum. Aff. 23 (4), 689–705. https://doi.org/10.2478/s13374-013-0158-9.
The Nation, 2022. 5 South Koreans arrested for telephone fraud in Chiang Mai. https://www.nationthailand.com/thailand/general/40022889.
The Nation, 2023. Attempted $897,000 fraud: yahoo boy forfeits N5m to Fed Govt. https://thenationonlineng.net/attempted-897000-fraud-yahoo-boy-forfeits-n5m-to-fed-govt/.
The Telegraph, 2024. Fake call centre busted, kingpin held in Assam. https://www.telegraphindia.com/north-east/fake-call-centre-busted-kingpin-held-in-assam/cid/1690956.
Times of India, 2018. Shaggy, India's most notorious call centre con, runs the show in NCR too. http://timesofindia.indiatimes.com/articleshow/67212348.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
United Nations, 2023. Online scam operations and trafficking into forced criminality in Southeast Asia: recommendations for a human rights response. https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf.
United States Attorney’s Office, 2024. Prominent Ghanaian “Influencer” sentenced to one year in prison for receiving romance scam proceeds. https://www.justice.gov/usao-sdny/pr/prominent-ghanaian-influencer-sentenced-one-year-prison-receiving-romance-scam#:~:text=In%20total%2C%20MONTRAGE%20controlled%20bank,fraudulent%20funds%20for%20the%20Enterprise.&text=In%20addition%20to%20the%20prison,in%20the%20amount%20of%20%241%2C387%2C458.

United States Department of Justice, 2025. Chairman of Prince group indicted for operating Cambodian forced labor scam compounds engaged in cryptocurrency fraud schemes. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged.

US Department of the Treasury. U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia. https://home.treasury.gov/news/press-releases/sb0278.

Wang, F., Topalli, V., 2024a. The cyber-industrialization of catfishing and romance fraud. Comput. Hum. Behav. 154, 108133.

Wang, F., Topalli, V., 2024b. Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. Am. J. Crim. Justice 49 (1), 145–181.

Whittaker, J.M., 2024. Towards an Understanding of Enablement in Online Non-delivery Fraud. Doctoral dissertation, University of Surrey.

Whittaker, J.M., McGuire, M.R., Lazarus, S., 2025. Conversations with deviant website developers: a case study of online shopping fraud enablers. Journal of Criminology. https://doi.org/10.1177/26338076251321844.

Youtube, 2020. Meet the Sakawa boys: ghana's internet fraudsters. https://www.youtube.com/watch?v=F1aGabH_PRo.

Yushawu, A., Jaishankar, K., 2025. Sakawa in Ghana: the influence of weak ties on economic cybercrime offender networks. Deviant Behav. 1–21. https://doi.org/10.1080/01639625.2025.2459681.

Button, M., Gilmour, P. M., Hock, B., Jain, T., Jesperson, S., Lazarus, S., Pandey, D., & Sabia, J. (2024). Scoping study on fraud centres: Ghana, India and Nigeria, ITAD, retrieved: https://eprints.lse.ac.uk/126338/.

Engle, T.A., Joo, S.H., Caudill, C. et al. An Examination of Cybercrime Trends Within the United States: Findings From the Internet Crime Complaint Center, 2015–2024. *Am J Crim Just* (2026). https://doi.org/10.1007/s12103-025-09885-w.

Herrmann-Pillath, C. (2013). Foundations of economic evolution. Cheltenham, UK and Northampton, MA: Edward Elgar Publishing.