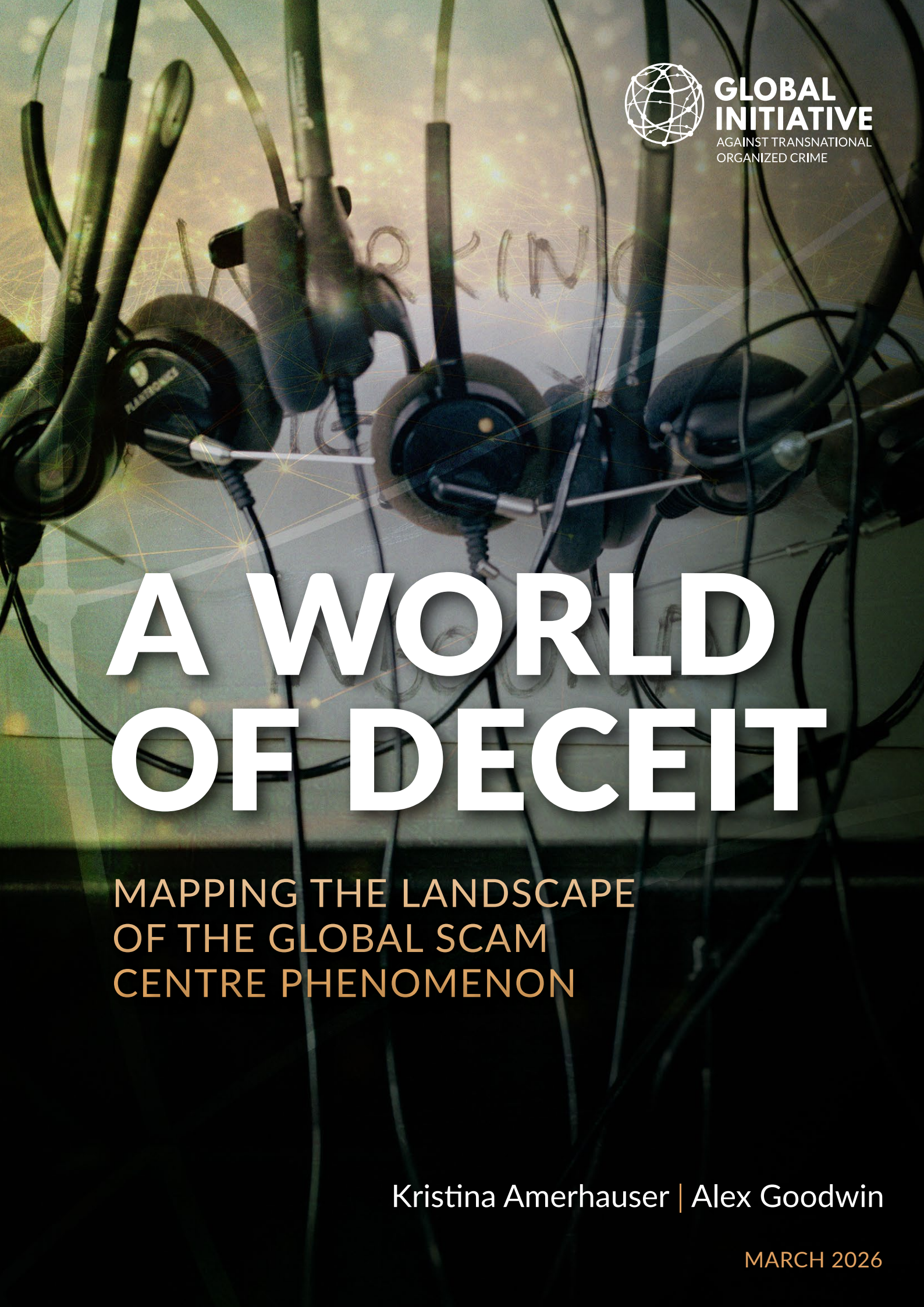


GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

A WORLD OF DECEIT

MAPPING THE LANDSCAPE OF THE GLOBAL SCAM CENTRE PHENOMENON

Kristina Amerhauser | Alex Goodwin

MARCH 2026

NOTE

This brief is based on qualitative and quantitative data and analysis collected by organized crime researchers based around the world. The authors would like to thank Daniel Brombacher and Sarah Fayes (input on Germany); C-Análisis (input on Colombia); Gabriel Funari (input on Brazil); Paddy Ginn (input on Pakistan), Aron Hyman (input on South Africa); Kingsley Madueke (input on Nigeria); Fatjona Mejdini (input on the Western Balkans) and Jason Tower (input on South Asia) for their hard work and unique perspectives that contributed to bringing this global phenomenon to life. The authors would also like to thank the many interview partners for their open and frank insights and contributions, and the Global Initiative Against Transnational Organized Crime's (GI-TOC) Publications team for their support.

ABOUT THE AUTHOR

Kristina Amerhauser is the head of the Mekong Observatory and leads the Mekong Network to Counter Transnational Crimes (MNET-CTC). She also co-leads the organization's work on illicit financial flows and conducts research on topics such as cyber scam operations, illicit financial flows, money laundering and corruption.

Alex Goodwin is a senior analyst at the GI-TOC's Eurasia Observatory, focusing on the impact of the Russo-Ukrainian War on organized crime and Illicit economies in the region.

Cover: © *Louis Quail/In Pictures via Getty Images Images*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

Executive summary **1**

Methodology 4

Ten key points 4

All shapes and sizes **6**

Prisons and pre-trial detention centres 7

Apartments, houses, villas and small offices 9

Compounds and major office operations 12

Six 'glocal' force multipliers **15**

Networked groups 15

Technology and crime-as-a-service 19

Money 22

Political protection 25

People 28

Geopolitics 31

Future risks and recommendations **33**

Recommendations 35

Notes 38

EXECUTIVE SUMMARY

Scams and fraud[1] have undergone a profound evolution in recent decades, becoming one of the most sophisticated and lucrative forms of organized crime globally. The playbook is as old as crime itself, centring around romance, investment and impersonation scams, but new variations are constantly emerging, including digital kidnaps, scams using malware and online sextortion. Many include a social-engineering element, meaning they are based on building personal relationships and victim manipulation. This personal connection also allows criminal networks to extract more money from a single person.

Today nearly everybody has a scam story: according to the Global Anti-Scam Alliance (GASA), in 2025, 57% of adults globally claim to have had a scam experience.[2] Scams have spread unchecked around the world, generating ever-growing amounts of illicit proceeds – money stolen from people like you and me. Estimates suggest that more than US$1 trillion was generated from scams and fraud in 2024, representing almost 1% of global GDP.[3]

Rather than focusing on the different types of scams and fraud, this report examines the scam centre as a distinct organizing unit. This report does not attempt to provide an exhaustive study of all scam centres around the world but rather examines the main global trends in the scam centre ecosystem that allow these centres and related operations to maximize reach, profit and efficiency. It looks at diverse economic models in four regions – Latin America, Europe and Eurasia, South East Asia and Africa, specifically West Africa and South Africa (see the map). Given that scam centres are adapting at pace, this report should be read as a snapshot in time with case studies used to point to similarities and differences in terms of operations, actors and linkages.

This report finds that while scam centres have unifying underlying principles, they are highly diverse in their physical footprints, organizational logic and economic models. The familiar image of a workforce seated at desks with headsets and a list of clients holds true in many places, but by no means all. Prisons around the world have long been incubators for scamming practices, as highlighted by our case study in this report on Colombia, where high levels of protection and a captive workforce create small but effective scamming units. Other scam centres are based in apartments, houses, hotels or modest office spaces – an approach that offers high levels of discretion and the ability to relocate quickly. The relatively small size of such operations should not give the impression that they are less harmful: not only can small outfits scam victims out of sizeable sums, but may in fact be part of much larger scam networks that essentially act as dispersed virtual scam centres with local nodes.

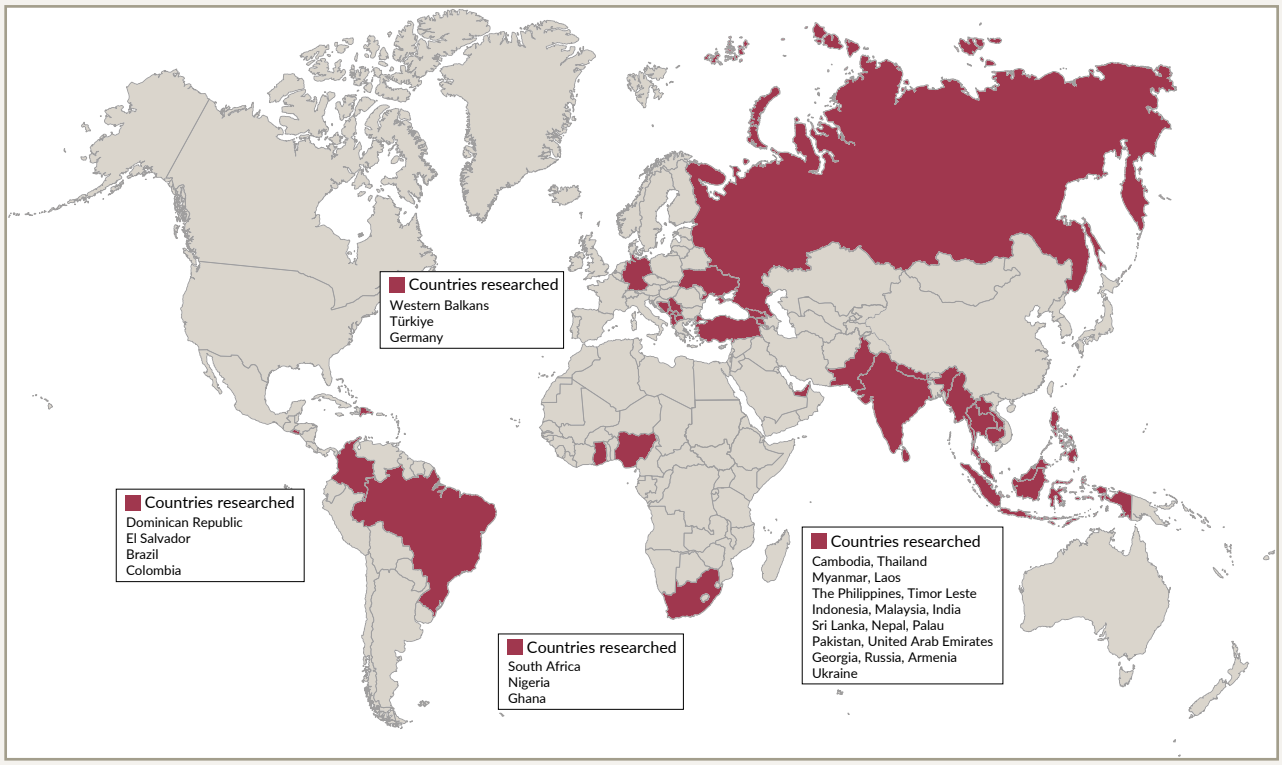


FIGURE 1 Countries researched during the course of this report.

Larger operations may have extensive office space, a clearly defined hierarchy and departments to manage different aspects of the business. Even at this scale, they still benefit from disguise, given that they often superficially resemble legal call centre outfits. Indeed, in many places scam centres are located or run their operations as part of online service companies, offshore gambling operations, special economic zones or legitimate call centres that provide customer support. The most extreme example is the scam compounds of South East Asia, which exert complete control over their workforce, a large part of whom are trafficked and forced to work in them. Such operations require high levels of political protection, but once this is secured, they can reap the rewards of industrial activity with little fear of repercussion. This is one the key findings of the report: that scam centres appear to thrive when corruption extends beyond low-level bribery to high-level political protection.

These operations are locally rooted in terms of physical infrastructure and protection, but they also avail themselves of global-level force multipliers. Technology has been one of the chief accelerants of the market, enabling scammers to reach victims anywhere in the world through a variety of means. Artificial intelligence is further pushing this envelope, enabling instant translation, deepfakes and voice cloning, app cloning and the instant generation of fraudulent documentation. Money laundering can draw on both local and global tools, from money mules and couriers to fintech and decentralized finance. Crypto, gold, cash and luxury goods are all vehicles by which scammers siphon off billions from victims around the world. Ultimately, scam centres are deeply connected to both global and local dynamics at the same time, making them 'glocal' operations in the true sense of the term.

Another key finding of this report is how pervasive scam centre activity is around the world. This is largely because the barriers to entry are low. Unlike many other forms of crime that are commodity-based (drugs, counterfeit goods) or human-based (human trafficking, migrant smuggling), scams require

little in the way of enabling infrastructure – all that is needed is a worker with an internet connection and an intent to deceive. There is no need to establish turf or expertise in a competitive marketplace: crime-as-a-service, whereby threat actors sell packaged tools or services used to deploy attacks, makes it easy for would-be scammers to acquire the components of a fledgling operation, from scripts to customer-relationship-management (CRM) software (which helps track victim data) and even potential employees.[4] Large datasets with contact information but also personalized profiles based on social media data underpin the scam industry and can be easily collected as well as purchased online and on the dark web. Thus, there is an ecosystem of enablers.

Another finding is that scam centres are replicable, due to their lack of logistical dependency. They can pollinate from country to country, driven only by an entrepreneurial management class that sees new opportunities and decides to establish operations in a new country, much like any multinational company. Staff can be easily sourced locally or from further afield, some drawn by promises of lucrative salaries, others trafficked and exploited for the purpose of forced criminality. Willing members of a diaspora can be harnessed as receiving nodes in illicit flows. And if local conditions turn against them, scam centres are easy to relocate.

These factors explain why many scam centres are part of larger networked structures with international reach, overseen by transnational syndicates. Interestingly, there appears to be little friction between rival players, except around payment channels and money laundering operations, suggesting that this market is in some ways unlimited. Whether this will remain the case is yet to be seen. Conceivably, as awareness of scams grows, the potential victim market may shrink, which may create increased competition among the actors involved. (Given the speed at which criminal actors innovate and come up with new types of scams, however, it is questionable if, and when, increased awareness may translate into a more competitive criminal market.) Another vector through which the illicit scam market might be 'regulated' is corruption and political protection, especially in places where high levels of corruption are required to operate. In these situations, state officials may function as 'licensors', granting permission to those who have the right connections and shutting down operations that do not. This has already been observed in Cambodia, Myanmar and Ukraine, for instance.

Illustration of a scam centre in Dnipro, Ukraine, February 2026. *Photo: https://t.me/ruslan_kravchenko_ua/577*

Scammers have also shown that they do not require a victim to have money to profit from them: by gaining access to the victim's credentials, it is possible to take out loans in their name. Others may target children, including through video games, and trick them into sending money or passing their parents' payment details to scammers they have met online. Therefore, there is clear potential for the illicit scam market to continue expanding.

This report shows how an approach to tackling scam centres that focuses on a single strand of the business will yield only limited results. Scam centres need to be understood as a diverse and continually changing phenomenon, with many different economic and organizational models operating around the world. They must also be understood as essentially 'glocal' constructs, availing themselves of online infrastructure, targeting victims globally and participating in transnational networks, yet also fundamentally responsive to and shaped by the local context where they have their physical footprint, which includes the nature and availability of political protection, relations with organized crime, cultural factors and the geopolitical situation.

In short, scam centres may be economically driven but they are also politically shaped. Only by responding to scam centres on all these levels can one of the most fast-moving and damaging forms of organized crime in the world today be effectively addressed.

Methodology

This report is based on multi-method research conducted in 2025. Preliminary consultations were held with the Global Initiative Against Transnational Organized Crime's (GI-TOC) 15 regional observatories to ascertain the main scam centre hotspots and key trends. Building on existing GI-TOC work on scam centres, particularly in South East Asia and Eurasia, 10 in-depth case studies were commissioned to achieve broad coverage of the illicit market. The research included interviews with a broad range of stakeholders, including those involved in scam centres, former convicts, local government officials, police officers, members of parliament and prosecutors working to respond to the issue. Journalists and members of local communities most affected by the crime were also interviewed. Although the GI-TOC attempted to validate the resulting information through additional open-source intelligence, the clandestine nature of scam centre operations makes systematic data collection challenging.

The case studies focused on known hubs, such as South East Asia, Nigeria and Eurasia, with exploratory research conducted in Latin America and countries with a reported presence of scam centres, such as Türkiye, Germany, Ghana and South Africa.

Ten key points

1. Scam centres provide a new perspective on the global illicit market of scams and fraud. As an organizational unit they present around in world in various shapes and sizes.
2. Scam centres draw upon six 'glocal' force multipliers that enable them to operate, scale, migrate and target victims with relative impunity: networked groups; technology and crime-as-a-service; money; political protection; people; and geopolitics.
3. Many scam centres are highly networked. Some pursue a multinational-style strategy, with core management opening new branches in different countries. Others are essentially dispersed scam centres, with small nodes of only a few people linked to a much larger operation. While it remains

unclear to which extent they learn from each other or are linked, there are indications that these networked operations allow lessons, techniques and technology to be shared, creating more efficient scam centres.

4. Technology is critical. At the most basic level, it allows scammers to reach people around the world at minimal cost. Beyond that, technology offers a range of tools for scammers to circumvent cyber defences; lure victims through deepfakes, auto-translation, cloned apps and fake investment sites; and access data that allows for precise social targeting of victims. Similarly, tools and infrastructure provided through crime-as-a-service providers are lowering the barriers to entry to the industry: today, a would-be scammer can buy everything they need off the internet, from data to scripts to software.

5. Money is handled through mules, crypto, fintech and cash and physical assets collected by courier. Victims, members of a diaspora, the elderly, the vulnerable and the young may all find their accounts being used by scammers to move money, in some cases unwittingly. The range of these approaches, often used in combination, means that tracing the money is a time-consuming endeavour for law enforcement as well as a race against time, though not impossible.

6. Political protection is fundamental for the scaling of scam centres, as seen most prominently in the scam compounds in South East Asia and extensive operations in Ukraine and Georgia. Globally, such protection can range from low-level bribery to the active collusion of corrupt state actors and political elites. This poses a major challenge to international law enforcement efforts, which may flounder against a wall of limited cooperation.

7. People are the lifeblood of scam centres. They may be drawn as willing and in some cases highly remunerated employees from the local population, or trafficked from abroad and forced to work in extremely exploitative conditions. The scale of the workforce is vast: some 300 000 people have been trafficked in the scam compounds of South East Asia. As well as being a human tragedy, there are questions as to the future of these trafficked scammers and whether they may fall back into scamming should alternative survival pathways not materialize.

8. Geopolitics also creates fertile opportunities for scammers, both in terms of generating confusion and urgency that scammers take advantage of, and in compromising coordinated international efforts to shut down scam operations. The rise of authoritarian rule across the world may further insulate scammers and hamper the efforts of civil society and investigative journalists who seek to expose them.

9. Looking ahead, there are three key risks: displacement, diffusion and deglobalization – all of which may assist scam centres to become more embedded in more places around the world. In addition, some countries may not directly be hosting scam centres but may be linked to the criminal industry by hosting money laundering or private sector enablers.

10. To tackle scam centres, it is vital to address the holistically interconnected nature of their operations as outlined in the points above. Single-strand approaches may shut down individual scam centres, but they will not meaningfully affect the operating environment in which these flourish. As with all forms of organized crime, if the business model remains sound, new participants will not be in short supply.

ALL SHAPES AND SIZES

Scam and fraud centres are a global phenomenon but they do not all share the same organizational logic or economic model. Around the world, scam hubs come in different shapes and sizes, with varying levels of sophistication, a diverse range of approaches and distinct behavioural traits. Local conditions often determine the shape and activity of scam centres, from the nature of protection they enjoy to the types of scams they perpetrate. Workers may be paid as much as 40% of the scam take in Nigeria, or be pressed deeper into debt bondage in the scam compounds of South East Asia.

Two of the most obvious differentiators are the physical space scam centres inhabit, and where they are located. In some countries, such as Türkiye, they fill only an apartment or office space; in others, such as in South East Asia, they fill multi-storey buildings in walled-off compounds or entire districts. Multiple shapes can exist side by side. For criminal networks, each iteration has its advantages and disadvantages.

Size does not necessarily correlate with impact. As some of the examples below illustrate, modest operations can still reap millions from their victims. Size can also be misleading: in South Africa, Nigerian confraternities[5] have created a model that sees small cells of up to six people networked into a much broader decentralised operation overseen by the confraternity. A lone scammer working from a modest house may be able to draw on the resources and expertise of a global organization. As internet connectivity spreads, scammers can work from anywhere, including villages and rural areas.[6]

Many countries are not dominated by a single model but host several operations as part of a diversified scamming ecosystem. Where prevailing patterns are evident, they may speak to the sector's consolidation, insomuch as a clear advantage has become apparent to working in a certain way, harmonising prevailing preferences of scale, visibility, workforce and protection. This is evident in the scam centres in India, South East Asia and in the use of business centres in many parts of Eurasia.

Depending only on business premises and an internet connection, this model has another advantage, in that it is easily replicable and enables networks to open new branches nationally and abroad. All that is required is a manager from the main network and employees (see below), access to the banking system (including money laundering service providers) as well as arrangements with local powerbrokers, if necessary. This managerial model is also highly efficient, in some places offering promotion for able scammers while ensuring core functions such as human resources, information technology and finance are handled as smoothly as in any legitimate business. Lessons and work can also be shared between different branches, creating a central pool of shared expertise.

Scam workers arrested in 2023 during a police raid on suspicion of running an online love scam syndicate in Indonesia. *© STR/AFP via Getty Images*

Scam centres are not rule-bound to maintain any particular model but may adapt as a result of changing operating contexts or political pressure. In South East Asia, for example, a recent wave of crackdowns may drive a move from large-scale compounds towards a lower-profile and more dispersed model, perhaps in new countries where awareness of scam centres is lower.

Type of scam centre	Advantages	Disadvantages
Prison/pre-trial detention centres	Captive workforce, close collusion between criminals and officials ensures protection.	Limited access to tech tools, limited workforce pool or opportunities to expand = limited reach.
Apartments/ houses/small-scale office space	Inconspicuous, low-cost, often drawing on local recruits, may come with 'built-in' security scammers can use.	This includes less organized operations that may also be more difficult to scale to different languages and target groups, but some may also be part of larger networked operations.
Large-scale office space and compounds	Provides space and facilities for highly structured operations with large workforces, meaning large reach. In compounds, maximum control of working environment, including use of trafficked workforce. Scale makes this form arguably the most lucrative model of scam centre.	Although resembling licit operations, large-scale office-based scam centres are conspicuous and rely on protection for continued operations. Compounds are highly conspicuous due to size and earnings, require high-level protection.

FIGURE 2 Scam centre types.

Prisons and pre-trial detention centres

Some of the simplest scam centres are found in prisons or pre-trial detention centres. Such scam centres have been seen in Russia, Ukraine, South Africa and Colombia, among other places. For those in charge of such operations, the benefits are obvious: a captive workforce often dependent on the hierarchy (criminal or official) for their quality of life while incarcerated, and fairly strong protection against prosecution. But such operations are also limited: scammers may have to rely on simple phone calls using supplied numbers, without being able to draw upon the arsenal of tech tools more sophisticated efforts use. Human resources are also constrained by the prison demographic – while scam centres on the outside can recruit men and women and those with specialised skills (such as languages or emotional manipulation), scam centres in prisons must make do with existing prisoners. Although these individuals can be highly effective scammers, without languages or tech it is more difficult to target victims abroad.

Colombia's prison scam networks

Scam centres in Colombian prisons are integrated operations that combine scammers working inside the prison with networks of mule accounts and payment collectors, suppliers of mobile phones and administrators of databases outside.

These scam centres exist within a context of high levels of structural corruption in which prisoners are subject to extortionate payments for multiple aspects of daily life, including access to food, a bed with a mattress, security for them and visitors, educational and job opportunities. The power exercised by prison guards over prisoners is extensive and, in many cases, almost absolute. This has given rise to a hierarchical criminal structure in which scamming is reportedly directed to and supervised by certain members of Colombia's National Penitentiary and Prison Institute's (INPEC) custody and surveillance corps.[7] These actors not only facilitate illicit activities but also act as strategic and financial partners within the system, leading the recruiting process of the callers, managing the stolen funds and acquiring the necessary equipment. They also appoint the so-called *pluma* (feather) or cell-block leader, an inmate tasked with coordinating, supervising and ensuring the execution of fraud and extortion activities within the block, as well as managing the day-to-day dynamics of each 'patio' or prison building.[8]

While exact make-up can vary, a typical criminal unit (see Figure 3) reportedly consists of one or two prison guards acting as coordinators, with a *pluma* overseeing up to six call operators – prisoners – working with a remuneration scheme according to their status in the prison system. These are approximated numbers based on interviews, but this structure has variations in size and agreements depending on the prison and other internal factors, such as the relationship between guards and prisoners. There was, however, consensus among interviewees that this is the most common pattern of organization of each criminal unit dedicated to prison extortion. People are not coerced into joining these structures; their entry is voluntary, motivated by profit. According to interviews with a wide range of stakeholders, key scamming hubs include the prisons of La Picota and La Modelo in Bogotá, Combita in Tunja, Picaleña in Ibague, Villa Hermosa in Cali, and Pedregal in Medellin.[9] These medium- and high-security facilities house prisoners who are considered highly violent and are serving long sentences, in many cases exceeding 40 years. This context significantly reduces incentives to desist from criminal activity, as the commission of additional crimes does not represent a meaningful marginal cost for individuals already facing lengthy prison terms.

Despite bans and frequent attempts to jam telecommunications,[10] the use of mobile phones among inmates exceeds 90%, according to the estimate of one former inmate.[11] Official figures from INPEC report that in 2025 alone, authorities seized about 35 000 mobile phones and SIM cards within the prison system.[12] External throw-ins and, more recently, the use of drones bring a steady supply to inmates.[13]

Alongside popular scams such as romance, fake service and family member in distress, prison-based scam centres in Colombia are also known for running fake extortion scams, playing on the pervasiveness of extortion in life outside the prison walls. In these cases, an additional role is incorporated in the structure: the lookout (*campanero*), who operates outside the prison, observing the victim, visiting the business or approaching the victim's daily environment to make the threat credible.

Although victim contact mechanisms remain basic and rudimentary, with no evidence of the use of artificial intelligence tools or sophisticated technologies to evade call tracing, scammers are adept at exploiting social media platforms such as Facebook, Instagram and TikTok, and employ social-engineering practices. According to an interview with an inmate, Facebook has become the most widely used platform, due to fewer restrictions on access to personal information and the ease of creating fake profiles using recycled photographs from other Facebook users.[14] Some foreign-national prisoners also provide contact information for individuals located outside the country, enabling transnational targeting. Oversight is basic but effective: information regarding the number of calls, their destination and other actions is entered into a kind of logbook, with profits distributed after the victim pays.

A parallel structure outside the prison handles the money once it has been extracted by the scammer. Money is often sent to low-value digital wallets[15] held by individuals

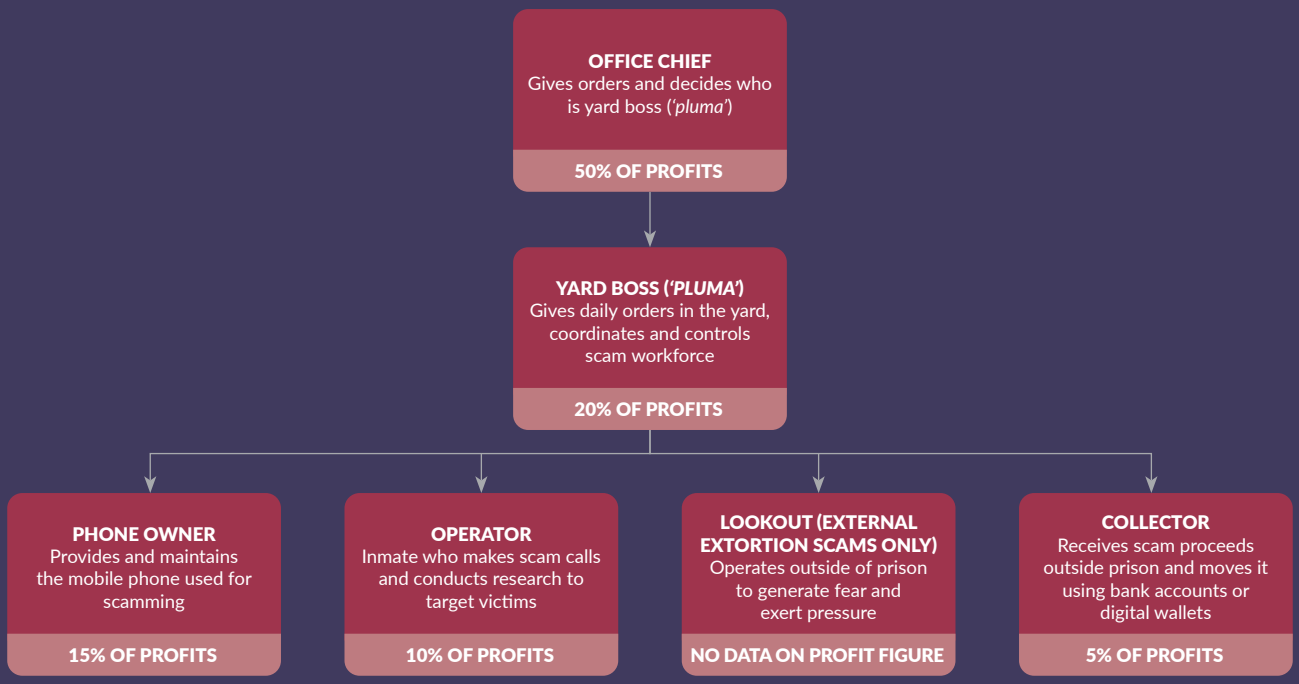


FIGURE 3 Organizational diagram of a scam group in a Colombian prison.

NOTE: This is an approximation of the structure, but different sources differ slightly as to the profit percentage taken by those called 'collectors' – the 5% estimate was provided by a former inmate, but in other estimates provided by banks that offer digital wallet products, identifying the transactional network responsible for collecting fraud and extortion related money as well as moving it, this percentage was 10%. No data was available for the percentage paid for the 'lookout' role.
SOURCE: C-Análisis.

known as 'droppers', who quickly forward it to 'collectors' in exchange for a commission – generally around 5–10%.[16] The process is extremely fast: funds rarely remain in the same account for more than five minutes, which significantly complicates tracing efforts, criminal attribution and judicial prosecution. Collectors consolidate the fragmented payments and send the amalgamated sums to formal bank accounts[17] that do not have amount restrictions (digital wallets have a maximum of US$3 000 a month). These bank accounts are overseen by ringleaders who manage annual cash flows ranging from US$250 000 to US$500 000.[18] To shield these funds from institutional oversight and potential investigations, they disperse the money among close family members away from the prison environment. ■

Apartments, houses, villas and small offices

In some countries, domestic spaces and sometimes small offices are used for housing scam centres. This model has distinct advantages: such operations are generally inconspicuous and the scale of the operation is unlikely to bring serious attention from international law enforcement, although arrangements might have to be made with local officials. When located in dense urban areas, these spaces provide access to individuals with digital and technical skills, and infrastructure such as offices and telecommunications networks.[19] In South Africa, houses are often equipped with high-tech security systems, often with electric gates and access control manned by private security guards and 24-hour CCTV monitoring, essentially outsourcing the scammer's security. Luxury apartments that host scam centres also often have their own private security in places such as Malaysia.[20]

The secluded location of villas – a modus operandi often used in Türkiye – helps avoid detection by neighbours or authorities. This is particularly needed for sex-related fraud schemes as it offers the privacy needed to stage convincing fake scenarios without immediate exposure, and the spacious layouts allow fraud operations to accommodate large teams working in shifts. Moreover, villas provide operational self-sufficiency – with full kitchens, private rooms and outdoor space – which reduces the need for occupants to leave the premises and risk drawing attention. For example, in an operation based in Denizli in July 2025, fraudsters ran scam centres across four provinces, targeting businessmen by offering escort services. The organization's hierarchical structure was directed remotely, and the group defrauded 35 victims of over TRY11 million (about US$274 000).[21] Short-term rental options and limited oversight in some rural areas also make it easier to operate anonymously and relocate quickly if needed.[22]

The close organizational resemblance to licit counterparts provides excellent disguise compared to other forms of organized crime where operations are notably conspicuous. Some scam centres run under the guise of legitimate businesses or are in fact legitimate businesses moonlighting as scam centres, blurring the distinction between legal and illegal. In many places, scam centres run their operations as part of online service companies, offshore gambling operations, special economic zones or legitimate call centres that provide customer support. For example, scam centres in the Philippines used licensed Philippine offshore gaming operators (POGOs) as front companies until their ban in 2024.[23] Since then, the POGO model has also spread to Sri Lanka, where individuals are registering online gambling or technology companies that are used as a front for scam operations.[24] In India, online scammers often hide behind legitimate businesses, particularly in the tech support industry. In November 2023, police discovered a web of related registered entities operating out of India with affiliates in the UK, US and Australia.[25]

In Türkiye, scam centres can also be found in apartments, units within high-rise buildings,[26] shopping malls[27] or office space in commercial buildings. Some of these appear to be bigger in scale, requiring higher levels of concealment. An expert on organized crime in Türkiye explained that shopping malls and office spaces are often preferred given their high anonymity, regular public movement and access to commercial utilities, further allowing scam centres to blend in.[28] For example, in November 2023, police in Mersin uncovered a scam centre disguised as an office that was targeting German citizens.[29]

Many of these scam centres are active 24/7 and have 20–50 workers operating in shifts to target victims in different time zones.[30] Workers have been found to live on site or close by to maintain a regular schedule. Recent police operations have shown a significant clustering of fraudulent activities in cities such as Istanbul, Izmir, Mersin, Antalya, Eskişehir, Ankara and Diyarbakır. These cities are not only economic and population hubs but are also known hotspots for broader organized criminal activity.[31]

In suburban parts of Brazil's two largest cities – São Paulo and Rio de Janeiro – scam centres were reportedly found in small office spaces located in conventional commercial buildings. The office spaces are reported to be leased for only a few weeks at a time to avoid police detection and the operations employ 30–40 people.[32] While much of this workforce is hired through job recruitment groups on Telegram, making them believe that they are set to work in legitimate telemarketing operations,[33]

others are recruited through personal links to the criminal network.[34] Some scam networks rent farmhouses and suburban lodgings through sites such as Airbnb for a maximum of a week at a time. The scam operators appear to bring their own internet routers and laptops and vacate the space within five days to avoid law-enforcement detection of their IP address.[35]

In the Western Balkans, fraud centres have been linked to legal outsourcing industries and customer services, and office spaces are commonly used. A 2023 case in Belgrade, Serbia, uncovered scam centres in modern-design offices selling non-existent cryptocurrencies. 'When you enter there, you have the impression of being in a state-of-the-art marketing agency,' commented a local prosecutor.[36] The modern working environment was accompanied by clean company documentation as all workers were registered and had their taxes and contributions paid. This made it difficult to discern it as a scam centre from the outside. In Kosovo, both in Pristina and Ferizaj, scam centres have operated in private apartments from where they ran fake investment platforms and trading.[37]

In El Salvador, scam centres are based in apartments and small offices in San Salvador, Santa Ana, Sonsonate and San Miguel. One recent large-scale scam was directed by a Colombian-led network, with Salvadorans serving as mules and logistics support.[38] In mid-2023, authorities detained more than 100 Colombians linked to improvised micro-finance outfits, advertising easy credit and locking borrowers into usurious terms before escalating into threats. When debtors fell behind, operators allegedly stole identities, opened bank accounts or requested cards, and moved funds. By July 2024, prosecutors stated that about US$20 million had been sent to Colombia with at least 170 defendants in the case.[39]

In Nigeria, scam centres – often known as Headquarters or Hustle Kingdoms (HKs) – have proliferated since 2020 across major cities, including Lagos, Abuja, Port Harcourt, Benin City, Asaba, Jos, Kaduna, Maiduguri and Kano. While many of these centres are operated by local networks, some of the larger and more sophisticated establishments are jointly coordinated with foreign actors from countries such as China, Indonesia, the Philippines and Lebanon.[40] Many of these scam centres are based in houses or rented apartments. Many operations are run by a 'chairman' who provides leadership and direction for the group, paying the rent for the apartment, feeding workers and sometimes paying for social outings to nightclubs and bars. The chairman also provides the type of fraud each member of the group should pursue and constantly assesses their efforts. Most chairmen operate on a 70/30% profit-sharing formula in favour of the chairman – highly generous to the workers by global scam centre standards: some even agree on 60/40%. In other cases, scam centres work more like cooperatives, where the rent is either shared between the workers or workers pay a percentage of their earnings to the person who owns the property. As one scammer said: 'Everyone is on his own but when you make money you have to give him something because he is doing us all a great favour by providing accommodation.'[41]

In South Africa, Nigerian confraternities have made strategic use of these types of small accommodation to create a networked model of a dispersed scam centre, enabling industrial-scale scamming to take place in a domestic footprint (see case study below: South Africa: Land of opportunity for Nigerian scammers).

Hotels and casinos

Cases of scam centres being run out of hotels and casinos have been reported in India,[42] Malaysia,[43] Sri Lanka,[44] Cambodia,[45] a Chinese-led group operating on the Isle of Man[46] and many more. Hotels are also sometimes used to house equipment (for example, SIM boxes) that allows scammers to call from overseas using local numbers, with at least two reported cases in Macau.[47]

Although hotels may give the impression of being short-term workplaces, in reality, they may host long-running operations. In January 2025, for example, authorities raided the Cocoro Hotel in Palau where 21 people had been listed as employees since 2023 or earlier. According to the Organized Crime and Corruption Reporting Project (OCCRP), citing Palau's National Security Coordination Office, many were in their late 20s and 'confessed to having never left the building in the past months, and sometimes years, that they have worked there.'[48] Two additional hotels suspected of being scam centres were also raided during the same period.

Similarly, in Cambodia, some scam centres are based in repurposed hotels, many of which were converted during the COVID-19 pandemic. These include the Long Bay Century Hotel and the Long Bay Casino Hotel within the Dara Sakor concession,[49] as well as the O'Smach Resort and Royal Hill, both located in the town of O'Smach. The O'Smach compounds were bombed by the Thai military during the border conflict in December 2025 and the area has been occupied since. Thai military brought foreign attachés and media to the area, allowing for a unique glimpse into scam operations and exposing rooms designed to look like Singaporean and Australian police offices, presumably to facilitate impersonation scams.[50]

Compounds and major office operations

At the upper end of the scale in terms of size and sophistication are scam centres located in compounds or occupying entire office floors in business centres. These operations are distinguished not only by their large workforces, but also for their use of tech, corporate structures (including human resources and finance departments) and distinct working cultures, which can range from 'boiler-room'-style environments to violence, both threatened and actual.

Some of these operations have emerged as copy-cats of a well-established (and legal) business process outsourcing (BPO) sector, which not only provides the pattern for how to work, but also helps generate a workforce that is experienced in similar roles and often has a high level of fluency in languages that are attractive to scammers, particularly English.

The Dominican Republic's legitimate BPO sector has grown steadily in the past two decades, supported by free-zone regions and a bilingual labour pool, with Santiago and Santo Domingo the main hubs.[51] Over time, a spectrum of call-centre formats emerged, most legal, some grey, and a minority criminal; today, a single office tower can host lawful and unlawful operations on different floors, with illicit floors hard to differentiate from legitimate BPO sites.[52] Illegal operations are highly organized and are typically multi-room offices with rows of headsets, role-segmented teams, printed scripts and visible supervision.[53] Tech does not play a large role, beyond caller-ID spoofing technology and VoIP auto-diallers, although the scams are notable for their sophistication in linking US targets with courier coverage, ensuring cash can be collected swiftly from victims.

Scam centres in Georgia, Russia and Ukraine have developed into highly sophisticated operations based in business centres and large offices. Investigative journalists have exposed several extensive

operations that have targeted victims in Europe and North America and have links with other scam centres in the region. These scam centres often make extensive use of technology, including deepfakes, fake trading platforms and document generation, to perpetrate long-running scams that can see individuals losing millions, especially in investment fraud.[54]

In addition, scam centres have been discovered using the facilities and buildings in special economic zones. This reportedly attracts less attention as the workforce is often from abroad and changes frequently. Also, law enforcement access to SEZs may be restricted. In South East Asia, some scam centres have also been discovered in self-declared SEZs or have presented themselves as part of China's Belt and Road Initiative (BRI) to bolster their legitimacy.[55]

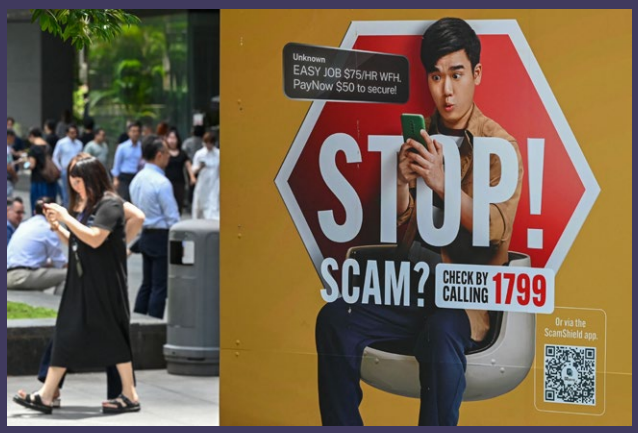
The large-scale scam model arguably reaches its apex in South East Asia, with walled-off complexes, large, trafficked workforces and highly coercive management practices, including violence and debt bondage. But such compounds are also difficult to hide. Instead, they are increasingly dispersing or based in areas of grey governance, often border areas, or in Myanmar in areas under the control of ethnic armed groups, where protection can be easily obtained. Indeed, in Myanmar, as cross-border scrutiny has increased, the compounds are increasingly moving inland away from border areas. Monitoring of Telegram groups in Cambodia also suggests that compounds are moving to residential and commercial office spaces to avoid raising suspicion, including when moving workers.

Scam compounds have also been reported in the United Arab Emirates, particularly close to Dubai and Ajman, the country's second largest city. According to the Humanity Research Consultancy, these have been clustered in industrial and investment parks, SEZs and as part of shopping and dining complexes. Like their counterparts in South East Asia (see case study below), they have been linked to China-linked criminal groups and are rife with exploitation for forced criminality.[56]

South East Asia: the apex of the scam economy

From remote regions to urban centres, scam centres in South East Asia are based in apartments, hotels, resorts, casinos and purpose-built compounds. Many of these buildings have been constructed or repurposed specifically to host criminal groups conducting illegal online businesses. The largest of these – cyber scam compounds – are highly sophisticated, operating industrial-scale operations that generate billions of US dollars in annual revenue. They generally feature extensive security measures – including gates, guard stations with private security and CCTV – internet, management, financial services and some form of protection from law enforcement campaigns. They are often self-contained, housing all the necessary facilities within individual buildings or compound walls. These can also include medical centres, karaoke and drug bars, restaurants and barber shops where workers can spend wages earned from perpetrating scams.[57]

Many scam operations in South East Asia are run by China-linked criminal networks, many of which had relocated to the region following domestic crackdowns.[58] They collaborate



An advertisement in Singapore warning the public of scam threats. *© Roslan Rahman/AFP via Getty Images*

closely with local elites and criminal networks to run the day-to-day operations. Criminal groups from elsewhere in Asia – notably of Japanese, Vietnamese, Malaysian and South Korean origin – have also been identified. Chinese actors often provide security at the compound, including through Chinese private security companies, with local armed groups or police sometimes supplementing these efforts with their own forces. Local business and political elites provide an umbrella of protection, decide where compounds are allowed to be established and operate, hold influence over law-making and law enforcement processes and more widely shape the criminal economy of the region.[59]

One notorious compound which attracted international attention was KK Park. Located in Myawaddy, a town in south-eastern Myanmar close to the Thai border, KK Park was a sprawling 210-hectare compound which in November 2024 hosted approximately 30 000 people. It was divided into six zones, each managed by a separate company. Individual scam syndicates leased or purchased space inside the zones for use in their day-to-day operations.[60] The broader Myawaddy area is controlled by the Myanmar military's Border Guard Force (BGF), which since 2024 has also referred to itself as the Karen National Army (KNA).[61] While administratively integrated into the Myanmar military, the KNA has semi-autonomous control over economic activity in Myawaddy and the BGF leader Saw Chit Thu has emerged as one of the central figures in Myanmar's scam economy. He has been sanctioned by the EU, UK and US.[62] Activities in the area and in and around KK Park are currently in flux, as the compound had been almost fully destroyed by January 2026. However, experts have argued that these crackdown efforts have been largely performative.[63]

It is important to keep in mind that KK Park is just one of many of such compounds across South East Asia: more than 200 compounds have been identified in Cambodia[64] and dozens of compounds similar to KK Park (including other 'scam cities' like Shwe Kokko Yatai New City[65]) have been identified in Myawaddy alone.[66] Despite their reliance on physical buildings, they are also highly mobile. For example, in Laos this criminal industry was concentrated primarily around the Golden Triangle Special Economic Zone but small compounds have now also been observed in Vientiane Capital[67] and Khammouane Province.

Across the region, there has been significant enforcement over the past months, partly driven by coordinated, consecutive and continued sanctions and travel bans by the US, UK, South Korea, Japan, Hong Kong, Taiwan, Thailand and others.[68] While it is too soon to evaluate the impact of these interventions, the crackdowns have led to significant displacement and questionable overall disruption. This is not only the case in Myawaddy, where new compounds have been spotted further inland in Myanmar, but also in Cambodia, where, following the arrest of Chen Zhi in January 2026, some compounds reportedly shut down, but many others proliferate and continue to recruit and/or have moved abroad.[69]

Scam compounds in South East Asia are underpinned by a sophisticated money laundering service industry and well-established crime-as-a-service providers. Cryptocurrencies and other fintech technologies, bank accounts, credit cards and cash are all regularly misused to transfer and launder illicit proceeds. Hundreds of payment guarantee and OTC crypto exchanges have been set up across these countries and in Thailand, Hong Kong, Taiwan, the Philippines, Malaysia and beyond to provide money laundering services to the scam syndicates. Often, compound owners themselves operate these services.[70]

As the underlying drivers and enablers of scam centres in South East Asia remain in place, the genuine success of crackdowns remains in question. Instead, operations are likely to become more discreet, more dispersed and less visible. They may also move to other countries in the region, including Indonesia,[71] Malaysia,[72] Thailand, Timor-Leste[73] and Sri Lanka,[74] where local scam centres have so far received less attention, presumably also because they are smaller in scale and rely less on trafficked victims as workers. For example, in October 2025, Thai police arrested 20 Chinese nationals involved in a scam centre based in a luxury house in Chiang Mai in the north of Thailand.[75] ■

SIX 'GLOCAL' FORCE MULTIPLIERS

Understanding scam centres through their physical infrastructure gives some sense of the variety of economic models in play. But scam centres are not islands: they are deeply connected to local *and* global dynamics at the same time.

This section identifies six 'glocal' force multipliers that have enabled scam centres to transform their diverse physical footprints into one of the most lucrative and harmful forms of organized crime in the world today: networked groups; technology and crime-as-a-service; money; people; political protection; and geopolitics.

Networked groups

Individual scam centres may operate independently and smaller networks may focus on specific countries, but many are part of larger networked structures that have not only national but international reach. The global tentacles of these operations and growing integration between local and transnational cybercriminal organizations marks a shift toward professional and globally networked cybercrime operations. While scam centres rely on physical buildings, the networked nature of the groups operating them makes them mobile and makes the set-up of scamming in new countries easy. Unlike other forms of organized crime, it is possible to start a scam centre with hardly any equipment, contacts or expertise. This expansion is also facilitated by choosing countries where protection can be bought (see 'political protection') or in diasporas that provide a sufficient shield from outside eyes.

For example, China-linked criminal groups that play a key role in South East Asia's scam industry have set up subsidiaries and conglomerates – and established less formal connections – in the Pacific, Africa and Latin America. This includes the World Hongmen History and Culture Association, which, according to the US Treasury, serves as a front for a China-linked transnational organized crime group established by a convicted 14K cartel leader.[76] The Hongmen Association has opened chapters in over a dozen countries, while reportedly maintaining close ties with the Chinese Communist Party and has, according to media reporting, routinely supported China's political objectives in South East Asia, the Pacific, Africa and Latin America.[77] Another example is the Cambodia-based and US- and UK-sanctioned Prince Group, which has established business interests in more than 30 countries.[78] Before the leader of the Prince Group was arrested in early January 2026, the conglomerate had hired a professional management team extending across the Asia region, and had made major investments in a full range of businesses around the world ranging from real estate to restaurants, financial institutions and even shares in Cuba's largest cigar company. This underlines that the reach of these organizations

goes far beyond their main areas of influence in South East Asia, a key factor to monitor as operations move or are displaced. In South East Asia, China-linked criminal groups cooperate with local criminal groups, local authorities and armed actors, including for the provision of security. For example, the United Wa State Army, a Myanmar ethnic armed organization, Laos national police and Chinese security have previously been reported to provide security in the Golden Triangle SEZ.[79]

Another example can be found in the Western Balkans, where scam centre groups have become professional and globally networked. This has been highlighted by a local prosecutor who explained that if scam centres were compared to a factory, 'Serbia would be the plant, Bulgaria would be some kind of IT department, Cyprus and Israel would be the management'.[80] Scam centres in Ukraine, Georgia and Albania have been found to be part of a sprawling network with common managerial figures and use of technology.[81]

In Türkiye, domestic and international criminal groups have been described as highly organized. Many of the higher-level criminals manage their scam centres remotely from abroad,[82] relying on local coordinators and a team of technical staff within Türkiye to run the daily operations. These local actors are typically in charge of recruiting staff, setting up the infrastructure and conducting the scams. In addition to homegrown operations, Türkiye has become a hub for international fraudsters, including from Russia, who bring advanced cyber capabilities such as malware deployment and data harvesting. These players team up with local groups who have networks across Europe and can access local protection.[83] Such groups reportedly avoid targeting Turkish citizens to reduce attention from local authorities.[84] There are growing indications that China-linked scam syndicates are adopting similar tactics, with Chinese police increasingly evidencing a shift towards what is referred to as 'foreigner butchering', which involves scam syndicates based in China or in Chinese border regions targeting individuals outside of the Chinese-speaking world to avoid detection and prosecution by Chinese authorities.[85]

Nigerian confraternities also run globally networked operations. In 2024, Interpol's Operation Jackal III targeted these networks in 21 countries. Money laundering operations were reportedly taking place in over 40 countries.[86] The international reach and increased professionalization of confraternities has been noted by police in Nigeria, where networks composed of nationals from China, Malaysia and the Philippines have established operational cells in major Nigerian cities, especially Lagos and Abuja. For example, in December 2024, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested 792 suspected cybercriminals operating from a seven-storey building on Victoria Island, Lagos. Among those arrested were 148 Chinese nationals, 40 Filipinos, two Kazakhs, one Pakistani and one Indonesian.[87] And in January 2025, the EFCC apprehended 105 suspects —101 Nigerians and four Chinese nationals — operating from an office complex in the Gudu area of Abuja.[88]

Nigerian confraternities have set up diverse operating bases in Nigeria, Ghana, South Africa (see case study) and elsewhere, establishing different types of arrangements with local powerbrokers. Scammers operating out of Nigeria reportedly pay bribes to local law enforcement to avoid arrests and/or be released,[89] and sometimes also have more structured arrangements where authorities receive a small percentage of illicitly obtained funds in return for ensuring scammers are not arrested.[90]

While some degree of learning, copying of techniques and cooperation among networked groups is likely, particularly through crime-as-a-service providers, the global extent of this remains understudied. Some exchange of expertise and experience has been observed among Nigerian confraternities who recruit and train young Nigerians and equip them with advanced technical skills and equipment to execute more sophisticated and large-scale online fraud schemes.[91] Some Eurasian networks are also highly coordinated, with a prohibition on local branches scamming citizens in the country where they are based.[92]

Chinese and Filipino nationals arrested in Nigeria also indicate connections with Asian criminal networks. According to one expert, it is possible that some of these may have been pushed out of the Philippines after the ban on POGOs, which was announced in July 2024 and came into force in October 2025.[93] It will be interesting to observe the activities of criminal groups following crackdowns in Myanmar and Cambodia in 2025 and early 2026. These may lead to relocation efforts and collaboration with scam centres and networks elsewhere.[94]

Involvement of organized crime in scam centres

While scam centres themselves are a form of organized crime, the actors running them have various profiles: businesspeople, opportunists, small groups, state-embedded actors and organized criminal groups. This in itself is interesting because, given the lucrative nature of scamming, it would be reasonable to assume that 'traditional' organized crime would have sought to take the business under its wing, but this is not universally the case. One of strongest examples of organized crime involvement is Ukraine, where scam centres are consolidated into several networks or 'grids', which are run by organized crime groups including Khimprom, which started as a producer and seller of synthetic drugs.[95] (Khimprom also allegedly runs scam centres in Europe and Myanmar.)[96] Nigeria's Black Axe, which has interests in drug trafficking and prostitution, also shows the high level of organized crime involvement. In South East Asia and the Pacific, China-linked criminal groups operating compounds have a long history of corruption, online gaming and gambling, wildlife trafficking and human trafficking. Some of the local business elites supporting these operations also have historical links to crime, including illegal logging, child labour and land grabs.[97]

In other contexts, these affiliations may be an illusion encouraged by scammers to increase the fear factor. In Brazil, for instance, arrested scammers often claim they are affiliated with major gangs in order to intimidate officers, 'but by the time their attorneys show up it is clear to us [the police] that these are criminals with no ties to the PCC or the CV [both major Brazilian organized crime groups], since these groups have their own specialized cohort of criminal attorneys. These guys have little sophistication to their actions. Their usual profile is of someone who will own a luxury BMW but will live in a house in the urban margins that lacks sanitation services'.[98] Despite evidence that large organized crime groups are not directly involved in funding or operating scam centres,[99] media outlets still often make a causal connection between the major gangs and scammers.[100] The networks behind scam centres in Brazil tend to be smaller-scale criminals that have historically specialized in hacking or cybercrime activities.[101] Similarly, in South East Asia and China, there appear to be many artisan scammers who operate smaller types of operations and which do not seem to have broader linkages to the vast networks running compounds.[102]

In a similar vein, prison scammers in Colombia typically impersonate members of high-profile armed groups, leading victims and media reporting to falsely claim that such threats are carried out by cartels or guerrillas.[103] However, there is no evidence that prison-based extortion is linked to other illicit economies or is carried out by actors such as the ELN, FARC dissident factions or the Gulf Clan, nor by organized crime groups such as the Tren de Aragua.

Organized crime may also play a more nebulous role. In Georgia, for instance, criminals did not manage scam centre networks but acted as providers of informal security.[104]

The intersection between 'traditional' organized crime and scam centres is therefore complex and by no means universal. This may be due to a perception that it is not core to their business – a response given by one consultant when asked why Latin American drug cartels appeared to have little involvement in scamming. However, this situation may also quickly change, as organized crime is not generally slow to act when there is easy money on the table. ■

South Africa: land of opportunity for Nigerian scammers

South Africa provides a compelling case of how easy it is for scammers to set up operations abroad and the benefits relocation may bring. Today, there is evidence that most scam centres in South Africa are run by organized crime groups from other countries, while smaller operations are run from prisons and by local gangs.[105] Cameroonian, Ghanaian and Israeli syndicates (the latter operating mainly 'boiler room' cold-call investment fraud schemes)[106] operate in South Africa, but the largest role by far is played by Nigerian confraternities.[107]

There are five Nigerian confraternities known to operate in South Africa, the largest of which is Black Axe, which has been in South Africa since at least the early 2000s and whose primary activities are business email compromise (BEC) fraud and romance scamming.[108] According to one senior US law enforcement investigator, South Africa is second only to Nigeria as the main hub for the proceeds of Nigerian confraternities linked to BEC and romance scamming proceeds.[109]

Scam centres operated by Nigerian confraternities are clustered primarily around Johannesburg and Cape Town, specifically in areas with large concentrations of Nigerian expats where support networks offer a 'soft landing' for new confraternity recruits coming to South Africa for the first time. Nigerian churches, both in Nigeria and South Africa, play a prominent role. According to one forensic investigator involved in numerous confraternity investigations, 'almost every single high-ranking [confraternity] member that we've taken through the court system, when you find out who's funding the senior counsel for a Black Axe member, it's always the Nigerian churches'.[110]

Scam centres in these areas are typically based in houses, particularly luxury houses in security estates, and hotel rooms or high-end apartments. Nigerian confraternities favour these types of high-security set-ups partly because they pose challenges to law enforcement teams attempting to conduct surveillance or gain access, buying valuable time for confraternity members to destroy evidence or evade arrest.[111] Confraternity members are even known to use their influence with security staff to gain access to CCTV footage they can use to identify undercover law enforcement units.[112]

The Nigerian scam centre model is distinctive, comprising small, self-reporting, highly networked cells that can draw upon sophisticated tech tools and the resources of a global organization. The number of employees is generally few – up to about half a dozen – although they reportedly compensate for this lack of manpower by their proficiency with technology, including AI tools such as deepfakes.[113] Members often only interact in person after hours at parties in upmarket nightlife venues where they bond with confraternity peers.[114]

This fragmentation serves a clear strategic purpose. According to one law enforcement investigator, Nigerian confraternities are 'way too clever' to centralise their scamming operations in one location or compound.[115] Instead, these micro scam cells form part of a larger collaborative network. Members communicate with each other under the oversight of the confraternity, sometimes across continents.[116] There is a clear division of labour – different members are tasked with establishing and maintaining technical infrastructure and fake documents, social media personas and other online infrastructure, or creating and perfecting scripts, or 'formats', which are blueprints perfected for successful scamming and which are shared between confraternity members during seminars.[117] For added credibility, Cape Town and Johannesburg-based members weave real-life experiences of living in these cities into their scripts.

Confraternity members pay money from scams and online fraud to the management structures. A substantial proportion of stolen money is moved to Nigeria, where the heads of all confraternities are located.[118] According to one law enforcement official, members tend to report their illicit earnings accurately because their earnings determine their status within the confraternities; the higher the position within a confraternity, the more downstream benefits a member will derive. This includes being given more 'territory' in which to conduct scams and expand their own networks. Confraternities will also hold members who withhold earnings to account. Without the confraternity's backing, Nigerian fraudsters will find themselves isolated in a foreign country and they will not be allowed to conduct scams or fraud in confraternity territory.[119]

Basing themselves in South Africa has a range of benefits for expat scammers, such as the elevated standard of

living in cities like Cape Town and Johannesburg, and the country's world-class internet and financial infrastructure. According to one cyber forensic expert: 'We often will see that the Lagos guys, when they do well, will begin to travel back and forth to South Africa regularly, in the same way that they'll go to South Africa and then to America, or Europe, or Dubai; in the same way that they'll go to Malaysia and then to Europe or America or Dubai from Malaysia. It's a stepping stone, if you will.'[120] South Africa also offers an opportunity to circumvent Western scrutiny over visa applications; the US, for instance, has strict policies for Nigeria due to concerns about organized crime members from the country moving to the US.[121] According to reports and law enforcement sources, some confraternity members marry South African women, often as part of a transactional arrangement, in order to fast-track getting a South African passport, which eases their onward movement to Western countries, as South African passports attract less scrutiny than do Nigerian passports.[122]

More practically, scammers know that asking victims to send money to South Africa will not raise the same level of suspicion and scrutiny as sending money to Nigeria. There are also apps, such as PayPal, that work in South Africa but not in Nigeria. In short, South Africa offers many advantages for relocating scammers and very little exposure to risk – a rare situation for migrating criminals. ■

Technology and crime-as-a-service

Scam centres are a hybrid crime that thrives on the use of technology to maximise psychological manipulation. Scammers target potential victims through telephone calls, mobile phone text messages, social media content, websites or other internet platforms. Therefore, their access to internet services and mobile networks is a prerequisite for the establishment of such operations. Raids around the world often recover similar hardware: computers, phones with SIM cards from all over the world, headsets, auto-diallers, caller-ID spoofing tools and voice-over-internet-protocols (VoIP), which enable the communication online.

While not all scam centres today work with sophisticated technology – indeed, many use the same tactics they have for years – it is tech availability online, on the dark web or on social media, that has facilitated scams to be conducted at scale and has lowered the barriers for others to enter. Thanks to crime-as-a-service providers that offer capabilities such as IT support, scripts, CRM software, websites and apps used in scams, beginners can now access ready-made tools and increase the volume as well as sophistication of attacks.[123]

The benefit of crime-as-a-service is that it can be accessed from anywhere, but what stands out is that many of the services delivered, such as datasets and SIM cards, are fundamentally local: their value to criminal groups is enhanced when they match their target audiences and serve to build trust.

The visual below is taken from a dark web shop and provides an overview of services that can be purchased. Services offered include access to specialized tools such as app cloners or 'spoofing as a service' – i.e. platforms that enable automated caller-ID spoofing.[124] They can also include scamming manuals such as 'grandparent scripts' which have been discovered in Germany[125] and the Dominican Republic,[126] handbooks on romance scams, which were discovered during raids on scam compounds in South East Asia[127] and material for impersonation scams, which were found in scam centre raids across Santiago and Puerto Plata in the Dominican Republic.[128]

Stage 1: In person

Before the mass adoption of telecommunications in the mid-twentieth century, scamming was largely in person, often involving direct participation of the scammer in the same physical space as the victim.

Stage 2: Telephone

Telecommunications allowed scammers to target their victims remotely and vastly increased the number of potential targets. But before the invention of Voice over Internet Protocol (VoIP), such scams were largely limited to the national level, due to the cost of calling overseas.

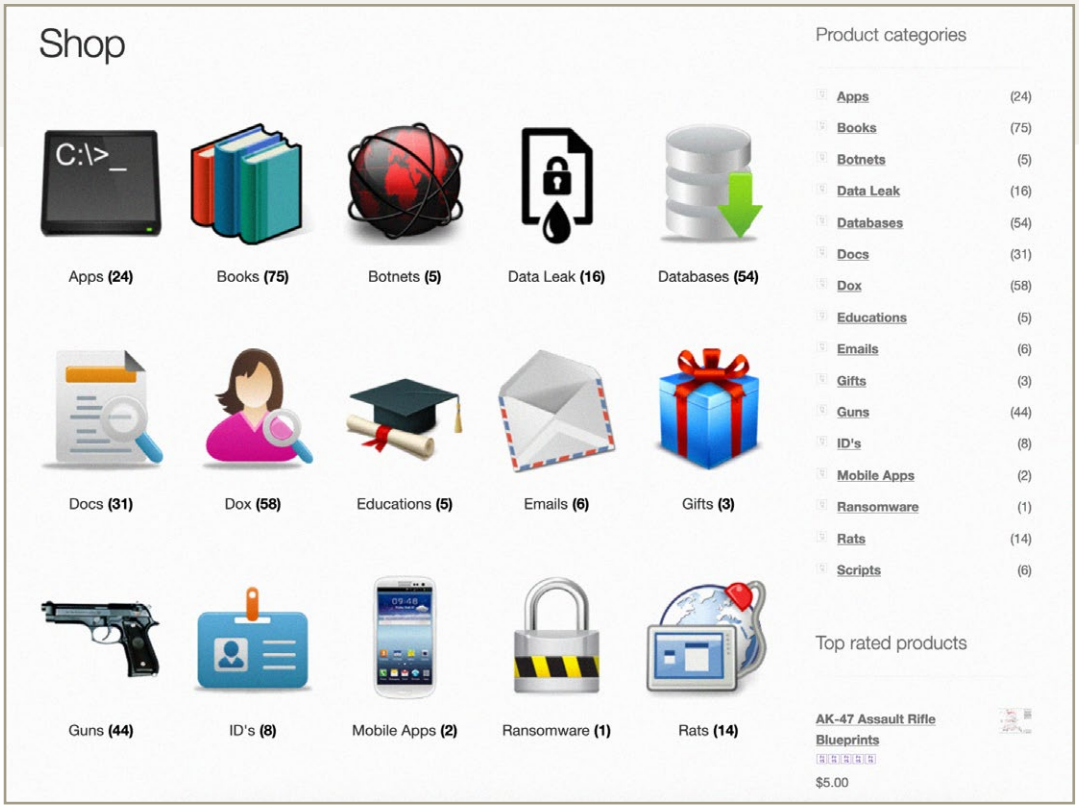
Stage 3: VoIP

VoIP and subsequent technologies opened up the entire world for scammers. All that was needed was an internet connection, some expertise in the victim's language and an ability to receive money at distance. This stage also bestowed greater protection for scammers, allowing them to operate in different jurisdictions from their victims.

Stage 4: AI

Artificial Intelligence (AI) opens up new possibilities, promising instant translation, deepfakes, voice cloning and the prospect of autonomous AI 'scam agents' working under the direction of a 'curator' scammer, who can tune scripts, map 'target areas', undertake 'vibe coding,' and, if necessary, step in to provide a human face. Under this model, there is no physical limit to the number of victims that may be targeted by a single scammer.

FIGURE 4 Four stages of social engineering scams: the exponential evolution of their reach.



Services such as data can be purchased on the dark web almost like any other legal commerce web shop. *Image: Dark Net Army, October 2025.*

Offerings also include data such as names, telephone numbers, stolen credentials, banking details or Facebook information. For example, in Germany, OSINT research showed that a database of 100 000 German phone numbers was available in bulk for as little as €5.[129] In another case, a list of 470 000 German phone numbers was sold for about US$10.[130] Phone numbers were also available on the dark web as part of broader personal data packages that include address, age and, in some cases, social security numbers. Typically, the more comprehensive the package, the higher the price on the black market – with complete identity packages being referred to as 'fullz'.[131] In one case such a full-information package for 100 000 German citizens was offered at a price of €500 000.[132] Criminal networks reportedly scan databases for old German given names that are no longer common (e.g. Hubert, Walter, Sieglinde or Gertrud), seeking to exploit the vulnerabilities of the elderly.[133] Identity information is also commonly sold in Türkiye – where authorities found detailed records of victims' identity documents, bank card information and transaction histories as part of investigations[134] – and across South East Asia.[135]

Criminal networks also purchase infrastructure such as hosting services for websites and apps, Starlink receivers in South East Asia or SIM cards. For example, the so-called SIM cartel relied on 40 000 SIM cards which were used to conduct calls and to create 49 million fake online accounts.[136] In October 2025, SpaceX reportedly cut Starlink communication links to more than 2 500 devices used by scam compounds in Myanmar.[137]

AI is supercharging fraud-as-a-service, as scam workers can use generative AI and deepfake technology to create convincing phishing content, clone voices or bypass biometric checks. It also helps to make the content more nuanced and context-specific. Some scam centres have been early adopters of AI, deepfake and voice-cloning technology to enhance their scams and development of fake apps. For example, deepfake videos were found at scam compounds in Cambodia[138] and also in South Africa, where AI prompts have been reportedly used to mask the voice of a scam worker (for example to make a male worker sound female) or to create authentic voices which match the accent and profile of the deepfake persona created by the scam workers.[139] AI is also developing to the point where scammers may to a certain degree be able to automate engagement with victims, using auto-translate functions to remove any language barrier. This model may also allow scammers to work on a vast scale, potentially spelling the end for workforce-heavy operations in the coming years and decades.

As is the case with organized crime elsewhere, scammers have been swift to overcome countermeasures with new solutions. In countries where anti-spoofing technology and legislation has been rolled out, such as Russia, fraud actors have begun using SIM boxes that allow scammers to connect to a local number from abroad. Bypassing verification systems is also no issue, with many companies offering temporary numbers for such a purpose at very little cost. In Nigeria, scammers reportedly use an app known as TextNow which provides users with international numbers, which they can then use to chat with potential victims and verify their accounts on social media and dating platforms.[140] Nigerian scammers also use VPNs such as IPVanish, CyberGhost, Total VPN, Express VPN and SurfShark to mask their true IP address. These VPNs have high speeds, extensive security features and some, such as Express VPN, can be paid for with cryptocurrency, allowing scammers to operate anonymously.[141]

The 'glocal' element can also be found in the use of social media by scam networks. While social media and communication platforms are used along the entire criminal supply chain – whether it is to recruit scam workers, communicate among group members, cultivate scam targets or facilitate the money laundering process – and while many of these platforms and apps operate globally, their use is often context-specific and requires targeted knowledge of who uses the platform, at what time and for

which purpose. For example, common dating apps targeted in Nigeria are known to users around the world and include Yahoo Personal, SinglesNet.com, Mingle2, Hi 5, OurTime.com, AdultFriendFinder, Hinge, Tinder, MeetMe, Kik, OxCupid, Zoosk and Craigslist.[142] Nevertheless, their successful use requires members to adapt to time zones and understand the local dating scenes. Other scammers use digital marketers to pair their social media scam adverts with a suggested audience based on profile and search terms, but even here, scam adverts are highly tailored to the target market, including, for example, deepfakes of prominent politicians, financial advisers or celebrities.

Going beyond digital technologies, local infrastructure-based technologies, construction and transportation also play an important role, particularly in areas where scam centres have become entrenched. For example, in South East Asia there are myriad private sector industries and suppliers that interact directly with scam compounds and companies.[143] These include providers of utilities such as electricity (scam compounds need continuous reliable power) as well as water, sewerage, telecoms (they cannot function without high-speed internet, be it WiFi or reliable mobile network coverage) and waste management, although some remote compounds are likely to have their own systems in place or use unbranded trucks for refuse collection. Furthermore, there is a whole set of transportation companies, including those to transport trafficked or willing workers to the compound upon arrival, food delivery services, warehouses and shipping companies that supply compounds with everything they need to function.[144] The massive profit stemming from the scam industry – some estimates put this at the equivalent of half of Cambodia's GDP[145] – have already significantly distorted national economies, with industries being partly co-opted into the scam economies. In many areas, it is likely that the scam industry has become an important local employer, and local businesses have become dependent on scam workers buying their goods and spending their scam proceeds.

Money

Money laundering is a globalized, professional, complex and multi-layered process that uses a range of financial technologies and transfer mechanisms which can be adjusted depending on the needs of the criminal network, the volume of illicit proceeds, the geography or the type of scam – meaning the way that illicit proceeds are generated (through bank transfers, in crypto or collected in cash).[146]

As previous research has noted, cryptocurrency infrastructure plays a central role.[147] This was confirmed by cybercrime experts who argued that it was at the heart of all cybercrimes.[148] Fake investment into cryptocurrencies or investment into fake cryptocurrencies have also been core scam techniques – there are many reports of scam victims who thought they were investing in cryptocurrency projects where quick returns are well-known.[149] As part of a scam, crypto wallets may be hacked, victims themselves may transfer cryptocurrencies to the scammer, scammers may coach their victims on how to convert fiat into cryptocurrency on legitimate exchanges and then transfer it to fraudulent platforms, or scammers may collect it in fiat and convert it into cryptocurrencies themselves. There are many scenarios and no single blueprint for this process. In South East Asia, once the funds are converted into cryptocurrencies (USDT has often been named the crypto of choice[150]), they are quickly moved through networks of coordinated accounts and passed through decentralized exchanges, fintech payment platforms, DeFI applications and mixers to scramble the funds between digital wallets.[151]

Cryptocurrencies are not only used for the laundering process but also to funnel money back to the scammers' home countries or to pay for operational expenses. For example, in Germany, payments

for data purchased on the dark web are almost exclusively conducted in cryptocurrency, with Bitcoin and Monero most used.[152]

While cryptocurrencies have become widely used by these criminal networks, the process is not limited to digital currencies alone. Criminal networks utilize a range of payment methods, including cash, fintech (such as peer-to-peer payment apps), bank transfers, credit cards and pre-paid cards to deposit, move and launder illicit funds. In many places they are not particularly sophisticated but rather fast and functional – but the payment mechanism selected is often linked to the local payment ecosystems where the victims and the scam workers are based.

This is visible in places such as Myanmar and Thailand where over-the-counter crypto-exchanges have proliferated and are used to convert USDT into fiat currency, as a means of moving proceeds into the formal economy. In other places local pick-ups and money transfers play a key role. For example, cash pickups in the US have been linked to scam centres in the Dominican Republic[153] – where authorities also seized lists of US area codes mapped to courier coverage in scam centre raids across Santiago and Puerto Plata.[154] These pickups are managed by so-called 'courier coordinators' who then move the cash onward to avoid banking scrutiny. In Nigeria, members of a scam centre noted: 'We don't get the money directly [but] we use a picker. Our picker is a very strong and smart man and he can collect money any which way that the client wants to send it. Sometimes he collects through Bitcoin, gift cards, PayPal etc. Once he collects the money he will convert to cash and send to another middleman who will then send it to us.'[155]

In Germany, some illicit proceeds are collected physically, with victims reportedly being lured into placing money, jewels or gold outside their houses or at a public spot to avoid physical contact with and potential identification of criminals. Experts consulted for this research explained that once the valuables are collected, the couriers immediately hand them over to more senior members of the network. The funds are then transferred through cash couriers or a Hawala system.[156] It appears that Turkish groups operating scams in Germany also specifically recruit for these 'collector' positions. One Turkish account with a German name was looking for collectors in Germany but only wants 'people with experience'.[157] Beyond certain skills and roles, other factors that suggest illegal intentions include non-standard business practices – such as insisting on WhatsApp-only communication, vague job descriptions, unusually high commissions, images of luxury items such as expensive cars or houses, or a high level of anonymization of the advertisers and alleged companies. Couriers collecting cash have also been reported in Russia and Belarus, sometimes travelling many thousands of miles to collect the proceeds.[158]

Mule bank accounts or e-wallets used to transfer or hold illegally obtained money play a crucial role in the money laundering process linked to scams. They are typically opened to facilitate local deposit, transfer and withdrawal of funds. These have been found to facilitate operations in Colombia, El Salvador,[159] South Africa, Nigeria, Türkiye, Thailand, Laos, Cambodia and elsewhere. After the funds pass through mule accounts, they are distributed to cryptocurrencies or other peer-to-peer networks.

For example, in Colombia, prison-based scam centres use a combination of low-value digital wallets, payment platforms and mobile applications. In many cases, networks recruit people for mule accounts who attract less suspicion from banks or other financial institutions, such as elderly individuals, students, persons with disabilities, Venezuelan migrants or female heads of household to open the accounts in exchange for about 10% of the profits. They are instructed to keep low balances in their accounts or e-wallets (far below any threshold that could raise suspicion with the authorities) and remain active for just a few months. They are used only to receive and transfer funds quickly (funds

rarely remain more than five minutes in the account): this way thousands of small transactions pass through these accounts and on to 'collector' accounts which function as temporary collection and concentration points for funds coming from multiple mules.

Nigerians involved in scam centres in South Africa are reported to collaborate with non-confraternity South African associates, who are paid to register bank accounts in their names. The confraternity provides these associates with burner phones on which they install a banking app linked to their account and hand the phones back to the confraternity. In this case, each phone is a mule account to which the confraternity has access and from which they move money around the world.

In other places, such as Türkiye and Thailand, scam networks target unemployed or economically vulnerable people to rent out their bank accounts in return for commission.[160] In Türkiye, a man received TRY8 000 (about US$180) to rent out his account.[161] In Thailand, people sell access to their accounts for THB 500–1 000 (about US$15–50).[162] However, not all mule account holders willingly allow their bank accounts to be used for illegal purposes. Many are believed to be deceived or manipulated. Sometimes the victims of romance or investment scams are further exploited by using their bank accounts as mule accounts.[163] In Thailand, people have reportedly been trafficked across the border to Cambodia for their bank accounts, while others were held captive in so-called mule stables in the country.[164]

Gaming or gambling platforms are also commonly used to launder illicit proceeds due to the high volume of transactions, the ease with which funds can be moved across borders and perceived legitimacy. For example, online sports-betting platforms have become an important conduit for illicit proceeds from scams in Brazil, which is the third-largest market in the world for sports betting, after the US and the UK.[165] In Pakistan, scam operations have been linked to online poker games where people had to register their credit card details, whereupon criminals stole their card information and money.[166] In Sri Lanka, researchers identified the presence of financial service providers operating inside major casinos that offered services from USDT, to cash, WeChat Pay, Alipay, most major credit cards and casino chips.[167]

Sometimes money is laundered using luxury items. In South Africa, as soon as money arrives in accounts owned by Nigerian confraternities, large amounts are withdrawn and immediately spent on, for example, luxury vehicles. This is an easy way for confraternities to quickly spend millions of South African rands, putting the money out of reach of the banks and ending the financial trail, thus making it more difficult for authorities to trace the money. These vehicles are then sold and the proceeds are deposited into crypto accounts or bank accounts in Nigeria. Expensive alcohol, brand clothing and jewellery are bought and sold in the same way.[168]

In some places, money laundering is facilitated as crime-as-a-service and has emerged as a market-place-type structure, where actors remain anonymous to others within the network. In South East Asia this includes sophisticated professional 'gateway' companies, which are trusted intermediaries facilitating communication and financial transactions between scam operations and money-laundering service providers in return for a fee. Using these gateway companies rather than laundering the money directly is likely to mitigate risks, while drawing on their knowledge of financial and legal systems in scam victims' countries.[169] What is striking is how networks of actors operate at the intersection of legitimate and illegitimate economies by using locally licensed crypto exchanges, registered fintech platforms and traditional banking services. Some competition between these money-laundering services has been observed, many of which are offered on Telegram channels.

Some of these laundering marketplaces may not only launder illicit proceeds gained by their local scam networks. Data from the Dominican Republic suggests that even when scam teams are based elsewhere, laundering marketplaces and over-the-counter brokers in the Americas may still be part of the financial chain.[170] Gateway companies in South East Asia are also known to facilitate money laundering from drugs or financial-sanctions evasion from North Korea.[171]

Once laundered, the proceeds are re-invested into running operations, stashed offshore in secrecy jurisdictions or converted into luxury items, precious metals and real estate. This creates a vicious cycle: greater profits enable these groups to expand their influence, which in turn reduces scrutiny of scam centres. With their growing wealth, the criminal groups may invest further into other types of crime and money-laundering-as-a-service infrastructure, generating additional profits that allow them to strengthen their influence and market position.

Political protection

Although scam centres may in many respects be able to draw upon global tools, they must invariably have a physical footprint within a certain country. This has consequences in terms of their geopolitical context (see below), but most of all it shapes their operating environment. In essence, their success and influence fundamentally depend on how well they embed themselves within local contexts, forge connections with local criminal groups and elites and how much protection they can buy/receive.

Such protection is a complex phenomenon. It can be low-level and purely transactional, such as police paid to turn a blind eye or to warn about upcoming raids. This was confirmed by a federal police officer in Brazil, who said that some degree of police protection was needed given the constant movement of scam centres. [172] In Nigeria, members of a scam network said: 'We don't pay to avoid raids because we're really hidden but when we get into trouble we pay them and they let us go.'[173] Nigerian confraternities in South Africa often have good relations with police officials from their local police station, which can help them get access to police dockets and early warning of possible law enforcement action against them.[174] Access to corrupt border management and Department of Home Affairs officials is also of key importance because most confraternity members are not in South Africa legally and may need to travel back to Nigeria or further abroad without being detected.[175] This has also been extensively documented in South East Asia.[176]

A wave of busts in Ukraine since the appointment of a new Prosecutor General in mid-2025 may spell a change in the fortunes of scam centres in the country, which have enjoyed a high level of protection. *Photo: Telegram, 23 February 2026, https://t.me/ruslan_kravchenko_ua/577*

Sometimes there are more structured arrangements between scammers and elements within law enforcement, who receive a small percentage of illicitly obtained funds in return for ensuring scammers are not arrested.[177] In Ukraine, some scam centres were reported to have a liaison person to handle the issue of protection with the police.[178] Figures between US$10 000 and US$15 000 a month were cited regarding the cost of such protection.[179] For this money, law enforcement may either leave the scam centre alone or give notice of raids, allowing employees time to prepare. After the police have departed, the scam centre can return to business.

Scam centres appear to thrive best when corruption extends to high-level protection of the criminal industry. This can be seen at both the micro and macro levels. At the micro levels, prison guards in Colombia direct, through intermediaries, certain segments of the prison population to conduct scams, benefiting from a captive and low-cost labour force. Higher-ranking guards who oversee multiple yards pocket about 50% of the scam profit.[180]

At the macro level, in South East Asia evidence not only points to the involvement of high-ranking law enforcement, but compounds are sometimes located adjacent to police stations.[181] In addition, an umbrella of protection appears to be provided by high-level politicians or military elites. For example, Cambodian senator Ly Yong Phat and his conglomerate have been sanctioned for their role in the scam industry.[182] And Chen Zhi, a well-known Chinese-born tycoon who purchased Cambodian citizenship and held a minister-level advisory role to Cambodia's then prime minister, Hun Sen, was arrested and extradited to China for his role in the criminal industry.[183] Both Ly Yong Phat and Chen Zhi also hold Cambodia's highest honorific title of *neak okhna*. As mentioned in the case study on KK Park, key political figures also provide an umbrella of protection to the criminal industry in Myanmar, where even the Deputy Minister of Home Affairs and Director of the Country's Anti-Scam Committee was recently stripped of his positions for accepting bribes from scam syndicate leaders.[184] Meanwhile, a similar situation is described in Laos.[185]

State-embedded actors also play an important enabling role in Türkiye, where protection has reportedly led to selective law enforcement against scam operations; scam cases involving politically connected individuals are often overlooked.[186] The Turkish government replaced over 95% of the police units dedicated to fighting organized crime and corruption in response to the 2013 corruption scandal and the coup attempt in 2016.[187] The loss of institutional memory and professional capacity, combined with a politicized police force, is seen as a key driver of rising criminality since 2016.[188] Like Cambodia, Türkiye offers a citizenship-by-investment programme which has been misused by fraud actors to establish themselves in the country and register business operations which provide a layer of legitimacy to their illegal operations. For example, a Swiss national who acquired a Turkish name and passport was accused of defrauding about three million people worldwide and stealing US$4 billion since 2019. In 2024, he was eventually discovered living in Istanbul.[189]

Taking the role of state-embedded actors in driving and facilitating organized crime as a proxy for political protection, the map shows the scores of the GI-TOC's Organized Crime Index in the countries where scam centres have been found and are discussed in this report. While this is only one factor – scam centres also need stability and consistent internet access, among other things – this may be helpful in considering why scam centres are able to take hold in certain places, and indicate where they might move next.

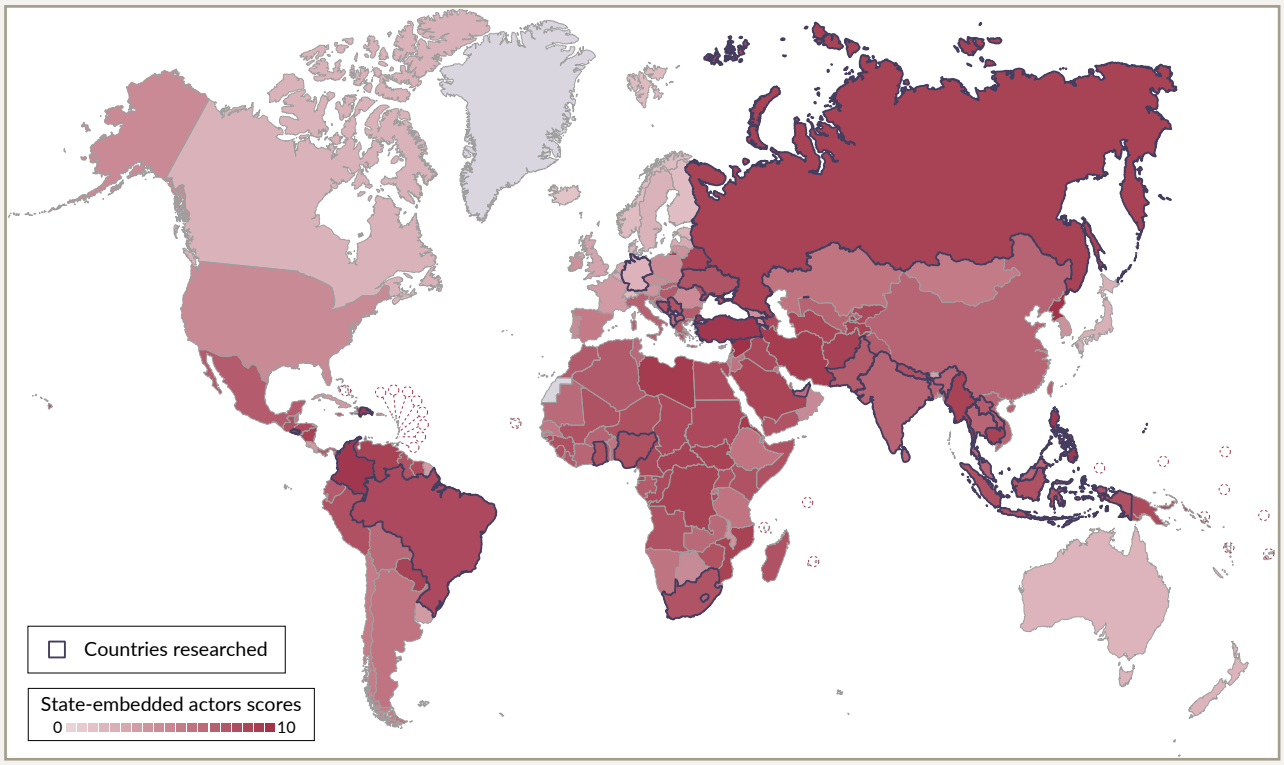


FIGURE 5 2025 Global Organized Crime Index scores of state-embedded actors, a useful proxy for the availability of local protection.

NOTE: Highlighted are the countries that were researched during the preparation of this report. In future, scam centres may be displaced to other regions where political protection is available, although considerations of stability and internet access are also important.

SOURCE: GI-TOC, Global Organized Crime Index 2025, https://ocindex.net/

Protected in Georgia

The scam centre economy in Georgia came to global prominence after investigative journalists revealed several large-scale operations with an unprecedented degree of sophistication and networking for scamming in the region, with losses among victims running into the millions. As in many other places around the world, underpinning this ecosystem was a strong protection economy that enabled the scam centres to work without harassment. This made investigations into scam centres by journalists highly challenging – and it was only a data leak that brought their inner workings to light. Even after the revelations, the wheels of justice have turned slowly and, to many observers, unsatisfactorily.

For example, the Morgan Group – a large scam centre established in Tbilisi in 2018 with links to the Milton Group in Ukraine and other scam centres elsewhere – was first exposed in 2020.[190] Georgian law enforcement initiated a case, announcing in September 2024 that the perpetrators had been arrested – timing that was seen as being in part politically motivated, coming as it did a month before the parliamentary elections.[191] However, these arrests did not translate into prison terms. Instead, the defendants accepted a plea agreement in June 2025 that saw them pay a fine collectively totalling €5 million, and they were released.[192]

Formulations of how this protection economy functions remain ill-defined. As in all such systems, it functions best when it appears invisible. Allegations may also have a political bias, particularly in light of the unpopularity of the governing party, Georgian Dream, at present. However, GI-TOC research in October 2025 heard that 'every call centre that operates in Georgia has a roof'[193] and the consensus among interviewees was that corrupt officials did not provide this

protection in exchange for money, but instead played a leading role in the establishment and functioning of scam centres.[194] (Although some were acknowledged to operate independently, making them more vulnerable to being shut down.)[195] In this model, protection is not a consequence of corruption, but a service provided by the key stakeholders.

Evidence for high-level state involvement came to light in October 2025 when a crackdown was initiated against the former inner circle of Bidzina Ivanishvili, the oligarch and former prime minister of Georgia who is the most influential figure in the country's political scene. Commenting on the events, one former diplomat said that 'the old government guys under investigation were the ones running the call centres operation'.[196] Ivanishvili was subsequently sentenced to five years in prison as part of a plea deal after being arrested for having 'secretly and covertly engaged in various types of business activities and received a particularly large amount of income of illegal origin'.[197] Prosecutors also alleged that the former head of the State Security Service had received bribes from scam centres in exchange for protection.[198] Criminal cases have also been launched against the 'thieves-in-law' and a former official allegedly directly involved in providing security to the scam centres.[199] However, there have also been reports of political motivation behind other arrests, including that of a journalist.[200] These events demonstrate how challenging it is to address corruption and protection within a state that is deeply compromised by such issues, and where such allegations may do more to serve a rival's career than clean up the system. ■

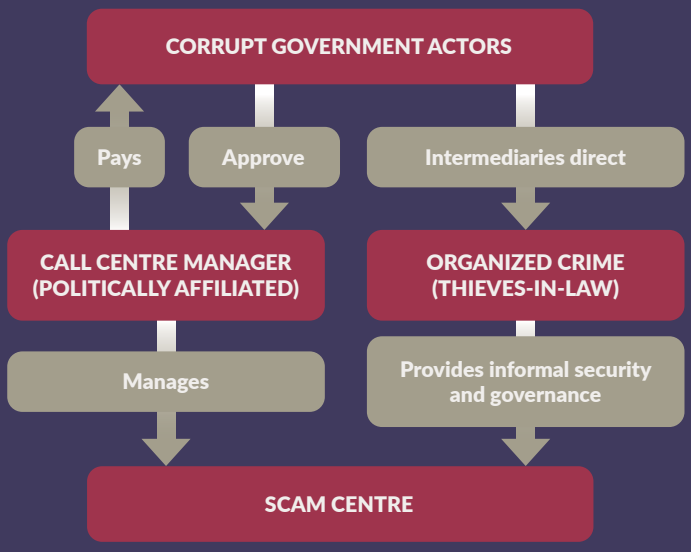


FIGURE 6 Model of the scam centre system in Georgia, based on October 2025 data.

SOURCE: Scammer's paradise: The scam call centre ecosystem in Eurasia, GI-TOC, forthcoming.

People

The scam industry involves many different roles, and scam groups are able to effectively match a very broad range of skill sets with these various roles, including at times through a comprehensive 'training' programme that involves sophisticated psychological and physical coercion and/or cult-like indoctrination. This means that scam centres can hire from an astonishingly wide pool, including detainees in prisons, trafficked workers lured from abroad, young, tech-savvy teenagers attracted by a well-paid job that requires zero experience, and members of organized crime groups.

Locals can provide a ready source of manpower, fast to hire and integrate. Locals are particularly useful for scammers in countries where there is a large pool of language skills and, in some places, a pre-existing market for call-centre-type work. This has been the case, for instance, in India, Ukraine, Georgia and the Dominican Republic, which all saw a boom in the legal call-centre sector as multi-nationals sought to lower costs by outsourcing non-core functions, generating a talent pool and

educational mindset, including an emphasis on learning English. Scammers can also recruit locals who have returned from overseas, as is the case with Turkish citizens who have spent time living in Germany as part of the large diaspora. These workers are particularly useful as they bring high-level language skills as well as detailed local knowledge of the target context, which can bestow enhanced plausibility on the scam.

Keeping it local may also be important in terms of trust, connection and operational security. In Brazil, for instance, some scam centres that operate in the suburban regions of Brazil's two largest cities, São Paulo and Rio de Janeiro, recruit employees by using the leaders' personal connections, employing 30–40 people in each scam centre.[201]

Scammers work in a global marketplace and take the same approach to recruitment. Disguising their operations, some scammers hire on regular job portals – using euphemistic descriptions such as 'service managers', 'IT services' or 'baristas' – or on Telegram, TikTok or Instagram, where the true nature of their business is often more overt.

One of the most obvious advantages to global recruitment is language facility: evidence shows that scammers do not just focus on major markets such as Chinese, English, Spanish or German speakers, but have diverse workforces capable of targeting relatively niche groups such as Slovakian, Hungarian, Korean, Japanese, Bahasa Indonesian and Thai. Employees who speak different languages and know about local conditions and cultural nuances can open up new potential marketplaces. In Ukraine, English and Russian may be the core desks in scam centres, but they have also sought workers with German, Italian, Czech and Slovak. Some scam centres have gone a step further and offer remote roles for people with the right languages. One job advertisement in Russian specified a need for workers in 12 languages, including Japanese, Chinese and Arabic, and offered to provide accommodation 'all over Europe'.[202] To obtain these skills, scammers also harness young people, language teachers and members of a diaspora (such as Turkish scammers recruiting among the diaspora in Germany).

Language skills are only part of the reason scammers look abroad for labour. They know they can take advantage of a dearth of well-paid jobs in certain parts of the world to attract skilled labour with superficially lucrative roles – some of the would-be employees even end up paying brokers for the privilege of acquiring such roles.[203] Once they arrive, 'employees' find they have become human trafficking victims, forced to scam under threat of violence and in debt bondage after various 'fines' are taken from their wages.

South East Asia is notorious for such practices. It is widely accepted that more than 300 000 people[204] from at least 75 countries[205] have been lured and trafficked into scam operations in Myanmar, Cambodia and Laos. In addition to victims of human trafficking, the workforce includes lower-level criminals as well as many employed are willingly.[206] The compounds themselves, or often the scam syndicates operating in these compounds, impose controls on freedom of movement and create deplorable conditions: when workers fail to meet targets or break draconian rules set by compound managers, they are subject to extreme torture, including food and sleep deprivation, beatings, rape and sexual violence, electrocution, water torture and other cruel forms of punishment, including being locked in cages with dogs. Murders are frequent, as are suicides.[207] The Office of the High Commissioner for Human Rights (OHCHR) has called it 'a humanitarian and human rights crisis'.[208]

While these levels of extreme violence on scam workers stand out in South East Asia, there is a growing list of locations to which young workers have been lured by false job offers and where they have been forced to conduct scams. This includes Nigerians and other West Africans who were lured

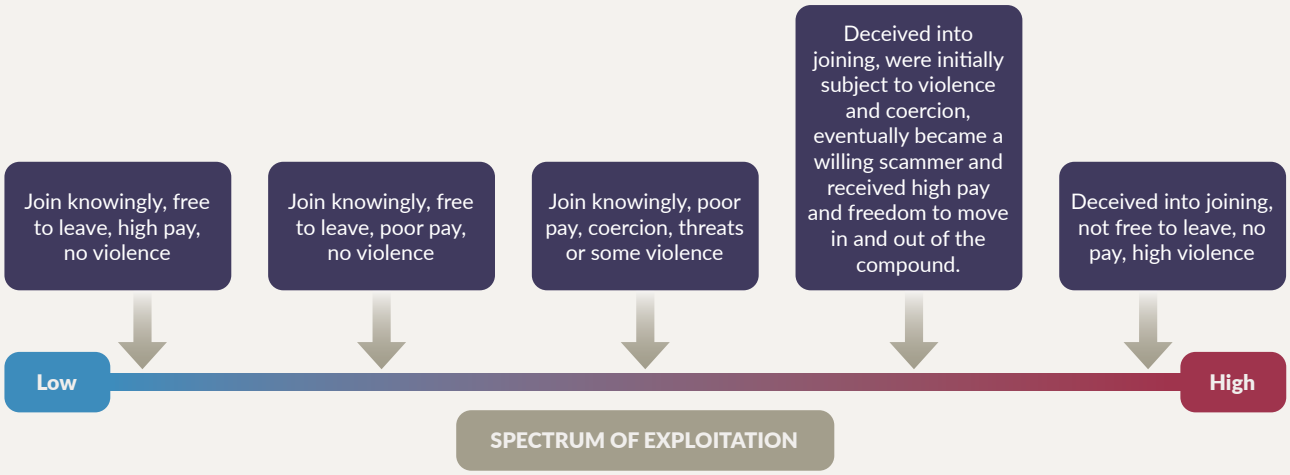


FIGURE 7 The spectrum of exploitation of scam centre workers.

to Ghana, forced to work long hours under surveillance, confined indoors, beaten and injured, who had their phones and passports seized and their food withheld.[209] In April 2025, 219 young individuals from across West Africa were rescued from such an operation in Oyarifa, Accra, Ghana.[210]

Leaders of scam networks operating out of Pakistan reportedly travel to Dubai to recruit workers from Bangladesh and Africa for the purpose of forced criminality. Once in Pakistan, they are held captive and have their passports taken away.[211] Scam compounds located in Dubai have also been linked to forced recruitment and exploitation.[212] In addition, local law enforcement in Sri Lanka and Nepal have referred to the existence of a 'visitor visa scam' or 'job scam' that involves tricking South Asians seeking overseas employment into travelling to the UAE without a work visa, only to discover on arrival that no job is available for them. These individuals are eventually recruited into scam centres locally or in South East Asia.[213]

Locals may also face similar pressures. In Ukraine, for instance, scam centres run by a certain organized crime group are known for their violent management style towards high-earning employees who want to leave.[214] In Nigeria, scammers reported punishment if they do not meet the monthly or quarterly targets but did not specify what this entailed.[215]

It is crucial to realise that coercion is by no means a universal principle in scam centres, nor does it appear to be necessarily linked to the type or size of scam centre. Many employees willingly do the work and some are even paid well. This also holds true in South East Asia where Lao, Myanmar or Cambodia nationals held in scam centres in their home countries almost always fall into 'low' categories of the spectrum of exploitation (Figure 7). In Georgia, for instance, scammers may earn much more than the average wage. The profit cuts for ordinary scammers may reach 40% in Nigeria, although this figure appears to be exceptionally high; ordinarily, the bulk of the takings goes to the head of the network. Other times, scammers themselves are deceived, promised extraordinarily high salaries before finding that these must be earned on commission, with a low base salary – which is the case in some scam centres in Ukraine.[216]

The divisions of experience shown in the spectrum of exploitation above are necessarily reductive, and different scam centres may function differently in the same country; it is also true that workers may move between different categories on the spectrum as their experience in the scam centre changes. Nevertheless, deceit is commonplace. Trafficked workers are exploited for the purpose of forced criminality, but many others find that promised wages do not materialise and advertised 'start-up' working conditions translate into coercion, abuse and control. As with scam victims themselves, there appears to be no shortage of those deceived by the promise of ready work in a world where jobs are scarce.

This spectrum also highlights the issue of the large and diverse pool of people engaged in this criminal industry in one form or another, who develop the knowledge and skills to conduct scams and who come into contact with criminal networks. This has important implications on the way forward, especially for those who have been repatriated after being trapped in compounds in South East Asia. Without job opportunities in the formal economy, they may use their new expertise to set up scams or link up with scam centres already operating in the country.

Geopolitics

Scammers are highly adept at exploiting geopolitical changes: each new crisis generates its own sense of urgency, need and confusion that scammers can manipulate to their own ends. This includes large-scale geopolitical changes, such as the COVID-19 pandemic or Russia's invasion of Ukraine in February 2022. During the pandemic, scammers created a universe of scams around financial relief, repatriation, medical issues and other associated needs.[217] The migration of people to a more online way of life – remote working, online shopping and social media – also vastly increased the target market for scammers.

Scammers also take advantage of geopolitical tensions. In some cases, this has led to an emergence of 'patriotic' scamming that focuses on foreigner scamming. For example, scamming of Russians by Ukrainians increased after Russia's invasion in February 2022,[218] but this is far from the only case. Scam calls from Pakistan to India reportedly increased following the Pahalagam attacks in April 2025.[219] A form of 'patriotic' scamming has also emerged in China that focuses on foreigner scamming – termed 'foreigner butchering' in Chinese. The degree to which this is a problem is underscored by the fact that the Chinese police have initiated public education programmes stressing that 'scamming foreigners is also a crime'.[220]

Connected to this is the issue of cross-border law enforcement cooperation. As political tensions between countries rise, cooperation inevitably suffers. At present, the nature of cooperation between target countries and the origin countries of major scam centre operations is varied. While China and Russia arguably pose the most significant cooperation challenges for Western law enforcement, China has at times exerted significant pressure on scam centres in South East Asia,[221] and in recent years Russia has cooperated with Kazakhstan, Belarus, Kyrgyzstan and Uzbekistan in joint operations against scam centres.[222]

However, as deglobalization advances, other countries may drift to new centres of gravity, creating an increasingly politicized climate for law enforcement to work in, with consequences for trust, information sharing and joint operations. For example, criminals may leverage geopolitical gaps or contestation in an attempt to evade prosecution.[223] In addition, the rise of authoritarian rule – with almost 40% of the world's population living under such regimes in 2024[224] – further erodes the space for cooperation

and effective law enforcement activity, especially in countries where the state is directly implicated in scam centres. In such contexts, the role of investigative journalism – so crucial in exposing scam centres protected by state actors – is also becoming more challenging. In Georgia, Kyrgyzstan and Russia, for instance, the passing of various forms of a 'foreign agents' law – superficially a regulation aimed to require civil society and media organizations to declare if they receive a certain proportion of funding from foreign sources, but in reality a tool to exclude and punish such voices – has had a chilling effect on investigative journalism, with organizations forced either to take cover or relocate overseas, reducing their effectiveness.[225] In South East Asia, journalists who have been at the forefront of raising the alarm bells on scam centres have been targeted and arrested, and representatives of NGOs as well as international organizations have opted not to speak out for fear of retaliation.[226]

Challenges faced by government authorities include a lack of established contacts with the country in question and an increasing list of countries to work with, straining capacity.[227] For example, some of the African citizens trafficked to Cambodia or Myanmar do not have embassies in these countries. Where such embassies do exist, they often have little experience in dealing with victim repatriation. International cooperation also frequently requires securing domestic buy-in, which may be difficult to obtain given concern around political optics.

There have also long been questions to which extent scam operations – and operations against them – can be instrumentalised as geopolitical tools. For decades, the Chinese government has sought to build influence across South East Asia, sometimes becoming entangled with organized crime. For example, China's quest for natural resources such as minerals and timber, and economic expansion through the BRI, had long provided an umbrella of protection to illicit activities long before the rise of industrial-scale scam operations.[228] This also means that while some levels of the Chinese government may disapprove of certain criminal activities, others may give tacit approval to certain actors and operations that align with broader Chinese interests in the region.[229] However, this tolerance appears to only extend as far as it benefits Chinese interests, with pressure or arrests occurring when the scale tips unfavourably. For example, the arrest and extradition to China of Chen Zhi, a US- and UK-sanctioned Cambodia-based tycoon, highlights China's influence in Cambodia and its ability to shut down scam operations. The timing was likely also linked to the realization that continued failure to act would result in other countries seizing the remaining assets and potentially arresting and trying Chen Zhi. If such a trial were to be conducted in the US or UK, for example, it would risk exposing the details of how the Prince Group had managed to evade Chinese law enforcement action for so many years.[230]

In Myanmar, the military junta has been vocal about a crackdown against scam centres, including bombing attacks carried out in November 2025. However, rather than a genuine crackdown, this show of force should be interpreted as political theatre,[231] as the targeted scam compound was in a region controlled by the junta's BGF and there was no attempt to mount an effective law enforcement response.[232] One theory as to the true motivation behind the attack may have been the junta's desire to negotiate a large slice of the scam-centre profits, i.e. to gain leverage rather than enforcement.[233]

Ultimately, geopolitics highlight how scammers continually seek to marry local dynamics with international trends, both for profit and protection. In this way, fraud is a crime that is not only economically driven, but politically shaped.

FUTURE RISKS AND RECOMMENDATIONS

As this report has demonstrated, the global scam centre economy is very diverse in terms of both geographic dispersion and organizational practices. It continues to change in response to global shifts and to innovate in terms of approach, use of technology and operational security.

Ultimately, scam centres are not a niche issue but a global concern: they inflict billions of dollars of losses and anybody can potentially be a victim. While awareness-raising campaigns have contributed to raising global alarm bells around the harms of scams, criminal groups have been quick to innovate and come up with new types of scams. The sophistication of AI tools – which will only increase – means that the plausibility of today's scams is extremely high, challenging the efficacy of awareness-raising programmes. Indeed, a voice-cloned message of a family member in distress may be close to impossible to distinguish from the real thing. It is therefore questionable when, or even if, this seemingly unlimited market will be faced with a shrinking pool of victims or confronted with increased competition.

Scam centres do not adhere to a single business model but come in many shapes and forms. However, while they look different around the world, common 'ingredients' remain. These components – some local and some global – mean that whatever form they take, they are easily replicable, making them ideal for networked models, which enable expertise and lessons to be shared and a coordination of efforts. For those scam centres without in-house expertise, crime-as-a-service provides many of the requirements, from tech to scripts to people. While it remains unclear to what extent networks already learn from each other or partner to expand their reach and income, at the moment a scammer can already copy-and-paste this model just about anywhere, within reason and with the benefit of local protection. The potential through further cooperation is massive.

Money laundering is as diverse and sophisticated as the scamming techniques. Crypto, fintech, money mules and couriers provide a global network that helps move illicit proceeds. Despite landmark seizures by the UK and US in 2025 in response to cyber scam operations in South East Asia,[234] much of this money is not recovered, and the labour-intensive efforts required to trace and seize scammed assets mean that many scammers are able to work with effective impunity.

Scam centres also benefit from superior camouflage compared to other forms of organized crime. There is no loitering on street corners, no suspicious packages to be secreted in cargo. Many scam centres operate in the homes and offices that we see in everyday life without realising what goes on behind closed doors. Their offices are next to ours, their fintech apps are licensed.

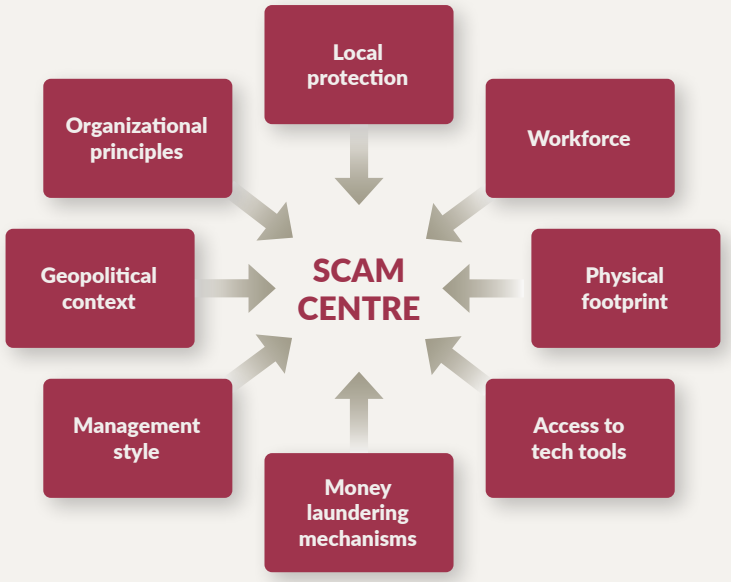


FIGURE 8 'Ingredients' making up a scam centre.

NOTE: Reponses that focus on one or two elements may produce results, but a truly effective response must encompass all the ingredients.

Ultimately it is clear that while scam centres are economically driven, they are also politically shaped. They exploit geopolitical shifts and changes to generate new scamming narratives and develop their tactics, as well as position themselves in places where they can operate to best advantage, safe from foreign law enforcement. They are a 'glocal' form of organized crime, able to operate globally with all the advantages of globalization, while at the same time being very locally rooted in an increasingly fragmented global order. Looking ahead, there are three areas of future risk:

- **Displacement:** As attention on scam centre activity increases in certain places, scam centres may migrate to more amenable climes. Given the current disposition, it is likely that serious actors will seek out places where political protection is easy to acquire and maintain, along with a certain political stability and good technical infrastructure. Countries that score highly for state-embedded actors on the GI-TOC's Global Organized Crime Index – one useful metric to measure the extent to which political protection is available – may be particularly vulnerable. Part of this diffusion may also be driven by those who have left scam compounds and who may potentially seek to begin their own line of work if legal alternatives are lacking. Given the low barriers of entry to the business, it only requires a few individuals with prior knowledge or the right connections to set up an operation that may quickly grow to have a significant impact, especially by drawing on scam solutions offered by crime-as-a-service providers.
- **Diffusion:** Large scam compounds attract a lot of attention; locking people up and abusing them even more so. That's bad for business. In future, scam centres may seek a lower profile, adopting models that avoid high concentrations of people and a conspicuous physical footprint. Already there are signs that scam centres are turning to more discreet working methods, whether it be renting working premises in less public areas, adopting more flexible workforce management structures (for example, allowing workers to work remotely) or adopting a more networked model, where a scam operation comprises a multitude of small, interconnected cells instead of one large central business. High levels of mobility allow scam centres to pollinate rapidly, like criminal versions of digital nomads. The smaller size of these operations should not be a cause for celebration.

Not only may they represent only the tip of the scam iceberg, but even small operators may be highly successful.

- **Deglobalization**: Organized crime pays keen attention to global affairs, and scammers are no exception. As the world continues to move towards a multipolar order, scammers will benefit from an expanded base and sources of friction. They will be early movers to exploit new rifts in law enforcement cooperation and the emergence of new grey governance zones, and will capitalize on new narratives. Scammers may also be harnessed by political actors for geopolitical ends, either for revenue generation or to seed narratives that blur scamming with disinformation. Scammers will also continue to thrive using tools that stand outside international instruments and regulations, such as decentralized finance.

Recommendations

Significant effort is already being put into tackling scams and fraud, by state, private sector and civil society alike. Such responses, however, are rarely focused on disrupting the architecture of the scam; they focus on awareness raising to prevent people from becoming victims, support for victims of human trafficking trapped in South East Asia's scam compounds, individual arrests, sanctions and seizures, takedown of websites and increased bank security checks.

While these measures have brought some scammers to justice, more can be done to tackle scam centres from a political economy standpoint, especially through the 'glocal' lens. Financial crimes and cybercrimes are the fastest growing criminal markets globally, according to the GI-TOC's Organized Crime Index, further highlighting the urgent need for new responses to these types of threats. Fundamentally, a holistic approach needs to address all the 'ingredients' that constitute a scam centre rather than focusing on one or two elements only. This report makes seven recommendations to disrupt the scam centre economy.

The Hong Kong Police Force hold a press conference about a joint operation to combat cross-border scams. Although much effort is being exerted to address the phenomenon, responses are often limited to law enforcement interventions such as arrests and raids. *© Chen Yongnuo/China News Service/VCG via Getty Images*

- **Treat scam centres as a form of organized crime.** As this report has shown, scam centres are far more than the practice of deceit for financial gain: they intersect with corruption and bribery, money laundering, cybercrime and in some places even human trafficking and violence. In practical terms, this means going after the leaders and middle management of criminal groups, rather than lower-level operatives, and increasing the penalties accordingly. This needs to go hand-in-hand with a better understanding of the harm of online and financial crimes, including their impact on international peace and security. Finally, treating scam centres as organized crime will require a systems approach which disrupts the enabling infrastructure, breaks down operating silos, promotes the sharing of experiences across sectors and includes a 'follow-the-money' perspective in all investigations.
- **Harmonize different tools of leverage, at home and abroad.** All law enforcement responses to organized crime would be helped by improved cooperation, data and information sharing and harmonization of legislation, and scam centres are no exception – not least since law enforcement from many different countries may ultimately be tracking the same criminals. Given the challenges in achieving this in a fractured political landscape, it is imperative that a variety of tools are deployed in tandem to put pressure on key scam jurisdictions, be it diplomatic, law enforcement or potentially economic. A greater sharing of suspect information and global target lists, for example, could increase the understanding of how criminal networks expand their operations to other countries; and a greater use of immigration blacklisting of key figures could intercept such actors before they have the chance to set up shop again, while support for investigative journalists can help expose corruption and provide a trusted outlet for data leaks. Coordinated and consistent international sanctions have already shown first successes, underlining the need for more and persistent pressure by a larger number of states on the criminal networks. Multilateral fora should also be maximised to exert pressure and constrain the working environment for scammers.
- **Build a truly global coalition against scam centres.** While most efforts are usually focused on places where scam centres already play a key role, this should not preclude a deep examination of the extent to which many countries that suffer from scamming may also be implicit in it, such as through dirty money being laundered through financial systems, assets owned, telecoms and internet technology misused, social media and diasporas coopted. Previous efforts to make private sector enablers of scamming more accountable – such as the UK's 2022 amendments to the Online Safety Bill (passed in October 2023)[235] – have lacked traction, and more pressure is required. Ultimately, an international response requires engagement with the countries that are already scam centre hubs as well as those that share some of the same vulnerabilities or are used for money laundering. Scam centres are a global phenomenon that need a holistic and networked response rather than a country-by-country approach.
- **Push for more private sector responsibility and accountability.** Technology and financial services are clearly enablers of the criminal market, but in many places other industries, including transportation, food and beverages or construction, have been linked to scam centres. As such, the private sector also has a crucial, though not uncomplicated, role to play in restricting – or in some cases maybe even denying – services and business to areas which are hubs for scamming. In addition, companies facilitating crime need to be made more aware of – and held accountable for – the misuse of the services they create and sell. The licensing process of fintech companies needs to be strengthened through greater emphasis on establishing beneficial ownership and more financial literacy needs to be built. There is a clear need to attempt to future-proof technologies to stay ahead of criminal market adaptations, including by leveraging private sector knowledge and data to anticipate and counter emerging threats.

- **Improve data reporting by challenging stigma and mainstream scam signalling.** Unlike drugs or the illicit wildlife trade, scams cannot be 'seen'. Victims have to come forward and report the cases to kick off investigations. At present, there is a critical dearth of such data, with an estimated 70% of scam victims not reporting the crime.[236] Improving the pipeline of data for law enforcement and prosecutors will be critical to painting a more comprehensive picture of how scam centres work. One key way of doing this will be to change the shame and stigma around falling victim to scams and create visible and easy-to-access forms of reporting in which victim, private sector and law enforcement can work collaboratively, together with extensive public awareness-raising programmes that provide information to help prevent people from falling prey to scams, and to contact the right authorities if they do. While some progress has been made and the private sector is already working to flag patterns of suspicious activity, the lightning-fast operations of scammers require new tools. This could include mainstreaming tools such as the Global Anti-Scam Alliance's Global Signal Exchange,[237] which supports data generation and sharing between key stakeholders. If this data is then shared with law enforcement, it also needs to include financial intelligence units so that they can immediately enhance transfer monitoring and look for suspicious patterns. Crypto poses a significant challenge in this regard, but the US-led US$15 billion seizure last year shows that it can be done. As general knowledge and access to crypto tools increase and the cost (in both time and money) of conducting crypto investigations declines, it may be that smaller taskforces are required to track and seize such assets. In addition, the media has a key role to play in scam signalling: rather than reinforcing stigmatization and shame, more victim-sensitive reporting is needed that details experiences, raises awareness around new types of scams and changing techniques, and challenges the way we talk about scams so that more people are encouraged to come forward.
- **Reintegrate former scammers into the mainstream economy to prevent proliferation.** Tens of thousands of trafficked former scammers are returning home, many to countries where jobs are in short supply. The temptation to turn to their old skillset may be strong in the face of economic hardship and potential social stigma, making it imperative that alternative employment pathways are established. Data from China suggests this is already happening. In 2024 alone, China reportedly repatriated and indicted over 78 000 people for online scamming, in total the number is likely as high as 120 000 convictions since early 2023. However, a criminal record makes it impossible for these individuals to find legitimate employment, leaving them with few options other than to fall back on their fraud-related skills. Some are now running small-scale, covert scam centres.[238] Some Indian nationals returning from scam centres in South East Asia have also returned to scamming, finding footholds in the country's already large domestic scam industry.[239] This underlines the need to monitor scammers that have returned home, as well as those trying to exit the industry, and to shape reintegration programmes to fit the skills and needs of these people.
- **Continue monitoring the trajectory of the scam centre economy.** As this report has shown, the scam centre economy is evolving rapidly, with many models in play. More research is required in regions where the phenomenon has not been strategically studied, such as Latin America, parts of South Asia and the Middle East, and the places where the money is laundered. There is a clear need to better understand how groups are networked and to what extent they learn from each other and cooperate. Knowledge gaps also persist around the role of private sector businesses as well as how operations evolve and adapt and where they go next.

NOTES

1 While the terms 'scams' and 'fraud' are often used interchangeably, there is an important difference: fraud is stealing money without the victim's knowledge (unauthorized), while scams involve tricking people into voluntarily giving up money or sharing information (authorized under false pretences). This report follows this approach and uses scams when there is a social engineering element. Fraud is also used as the umbrella term when this distinction is unclear. See: *What's the Difference between Fraud and Scams?* OnPoint. Community Credit Union, 30 September 2024, https://www.onpointcu.com/blog/whats-the-difference-between-fraud-and-scams/.

2 GASA, Global state of scams, 2025 report, no date, https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_94a72790e5cf4d24bc59e521872a4377.pdf.

3 Sam Rogers, International scammers steal over $1 trillion in 12 months in global state of scams report 2024, GASA, 7 November 2024, https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai; Global GDP in 2024 was estimated at US$111 trillion, meaning US$1 trillion is equivalent to 0.9%. See Global gross domestic product (GDP) from 2000 to 2030 (in trillion US dollars), no date, https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/.

4 Crime-as-a-service usually includes various components, for example, Europol lists infrastructure-as-a-service, data-as-a-service, pay-per-install services, hacking-as-a-service, translation services and money-laundering-as-a-service. See EC3, The Internet Organised Crime Threat Assessment (iOCTA), chapter 3 – Crime areas, 2014, https://www.europol.europa.eu/iocta/2014/chap-3-1-view1.html.

5 Confraternities refer to student-founded groups within Nigerian universities that have become major organized crime networks. Some well-known confraternities include the Vikings, Black Axe, Eiye and the Buccaneers. See Helen Oyibo, Nigeria's campus cults: Buccaneers, Black Axe and other feared groups, BBC, 2 June 2020, https://www.bbc.com/news/world-africa-52488922.

6 WION dispatch, 2302 Villages flagged, 6pm, 24 February 2026, https://www.facebook.com/WIONews/videos/2302-villagesflagged-6pm/1691211075180042/; Snidgha Poonam, 'Scamming became the new farming': inside India's cybercrime villages, *The Guardian*, 30 October 2025, https://www.theguardian.com/technology/2025/oct/30/scamming-became-the-new-farming-inside-india-cybercrime-villages.

7 Interview with a former inmate of La Modelo and La Picota, Bogotá, 30 December 2025.

8 Interview with a former inmate of La Modelo and La Picota, Bogotá, 30 December 2025.

9 Interview with the Attorney General's Office, Attorney General's Office Bunker in Bogotá, 7 January 2026.

10 Most penitentiary facilities are located within densely populated urban areas, which significantly hinders the effective isolation of communications. The blocking of mobile phone signals not only presents major technical challenges, but also legal constraints, due to the impact on surrounding neighbourhoods and the lawsuits filed because of service interruptions. Currently, INPEC faces fines amounting to about COP 58 billion (US$15 million), stemming from lawsuits filed by residents living near prisons, because of the installation of wide-range jammers that affect external connectivity. Some complainants have claimed headaches and other health impacts. Moreover, many of the installed jammers rely on obsolete technologies designed to block 2G and 3G signals, ineffective in jamming mobile communications operating primarily on 4G and 5G networks.

11 Interview with a former inmate of La Modelo and La Picota, Bogotá, 30 December 2025.

12 Interview with an INPEC official, INPEC offices in Bogotá, 7 January 2026.

13 Carlos López, Use of drones in prisons: the new method for smuggling drugs and cell phones, as denounced by the director of the National Penitentiary and Prison Institute

(INPEC), *El Tiempo*, 7 September 2025, https://www.eltiempo.com/justicia/delitos/uso-de-drones-en-carceles-la-nueva-modalidad-para-ingresar-drogas-y-celulares-que-denuncia-el-director-del-inpec-3488519; Rueda Figueroa and Danna Valeria, Drones were used to unload drugs and cell phones inside the cells of the Palogordo prison in Santander, *El Tiempo*, 3 June 2025, https://www.eltiempo.com/colombia/santander/con-drones-pretendian-descargar-droga-y-celulares-al-interior-de-las-celdas-de-la-carcel-de-palogordo-en-santander-3459881.

14 Interview with a former inmate of La Modelo and La Picota, Bogotá, 30 December 2025.

15 These digital banking tools were designed to promote financial inclusion; their simplified onboarding models allow virtually anyone to open a low-value digital wallet with minimal requirements: typically basic personal information, a national ID, biometric validation and a mobile phone number.

16 Interview with financial institutions, Bogotá, 22 January 2026.

17 These low-value digital wallets have a maximum transaction amount of COP11 million (around US$4 000) a month. Moving the money to traditional saving accounts is a crucial step for the extortion cells. They need multiple stages in the financial system to collect larger amounts of money and need to be able to take it out before banks stop the transactions or freeze the accounts.

18 Interview with bank representatives, Bogotá, 22 January 2026.

19 Focus group study with five financial crimes investigators, August, 2025.

20 See last paragraph of T N Alagesh, Scam call centres move to remote budget hotels to avoid detection, *New Straits Times*, 1 December 2025, https://www.nst.com.my/news/regional/2025/12/1327637/scam-call-centres-move-remote-budget-hotels-avoid-detection.

21 *Eskort ilanı için lüks villaya çağrı merkezi kurup 11 milyon dolandıran 17 şüpheli tutuklandı*, Sabah TV, 5 July 2025, https://www.sabah.com.tr/video/yasam/eskort-ilani-icin-luks-villaya-cagri-merkezi-kurup-11-milyon-dolandiran-17-supheli-tutuklandi-video.

22 Interview with a former police officer who worked in the Anti-Fraud Bureau, August 2025.

23 Senate of the Philippines, Press release, Stop POGOs now – Hontiveros: POGOs used as legal cover for scam hubs, 30 May 2023, https://legacy.senate.gov.ph/press_release/2023/0530_hontiveros2.asp.

24 Interview conducted in Colombo, Sri Lanka, February 2026.

25 ED files prosecution complaint against Met Technologies director, 8 others, Business Standard, 18 November 2023, https://www.business-standard.com/companies/news/ed-files-prosecution-complaint-against-met-technologies-director-8-others-123111800635_1.html; Jack Meegan-Vickers and Kristina Amerhauser, Scam wars: Joint US–India focus on cyber scams is a chance to curb a global fraud epidemic, GI-TOC, 21 April 2025, https://globalinitiative.net/analysis/joint-us-india-focus-on-cyber-scams-is-a-chance-to-curb-a-global-fraud-epidemic/.

26 *Çağrı merkezi kurup dolandırdılar! İşte operasyon anları*, BursadaBiz, 14 May 2024, https://www.youtube.com/shorts/mZMsh7h8PTg.

27 *Çağrı merkezi dolandırıcılarına operasyon kamerada*, IHA, 19 October 2016, https://www.iha.com.tr/haber-cagri-merkezi-dolandiricilarina-operasyon-kamerada-595071.

28 Information provided by an organized crime expert working in Türkiye, September 2025.

29 *Dolandiricilik Şebekesini Mersin Polisi Çökertti*, Mersin Emniyet Müdürkügü, 21 November 2023, https://www.mersin.pol.tr/21-11-2023-dolandiricilik-sebekesini-mersin-polisi-cokertti.

30 Interview with a former police officer who worked in the Anti-Fraud Bureau, November 2025.

31 Interview with a former police officer who worked in the Anti-Fraud Bureau, August 2025.

32 Interview with a police investigator from the São Paulo Civil Police fraud division, September 2025.

33 Interview with a cybercrime researcher, September 2025.

34 Interview with a cybercrime researcher, September 2025.

35 Interview with a cybercrime researcher, September 2025.

36 Naralija Jovanovic, *'Sve je izgledalo kao legitimni biznis': Beograd u srcu istrage o kripto prevari*, 2 March 2023, https://www.slobodnaevropa.org/a/beograd-u-srcu-kripto-prevare/32296388.html.

37 *Mashtrimi i 350 personave nga Gjermania përmes "Call Center" në Kosovë, policia gjermane del me detaje*, *Gazeta Express*, 5 December 2024, https://www.gazetaexpress.com/mashtrimi-i-350-personave-nga-gjermania-permes-call-center-ne-kosove-policia-gjermane-del-me-detaje/.

38 *Fiscalía ordena captura de estructura de colombianos que utilizaban a salvadoreños como mulas financieras para lavar dinero proveniente estafas y hurtos informáticos, entre otras actividades ilícitas*, Fiscalía General de la República (FGR) Prensa, 18 July 2024, https://www.fiscalia.gob.sv/fiscalia-ordena-captura-de-estructura-de-colombianos-que-utilizaban-a-salvadorenos-como-mulas-financieras-para-lavar-dinero-proveniente-estafas-y-hurtos-informaticos-entre-otras-actividades-ilicitas/.

39 *La Fiscalía salvadoreña presenta requerimiento contra 110 colombianos acusados de lavado*, Swissinfo, 27 July 2024, https://www.swissinfo.ch/spa/la-fiscalía-salvadoreña-presenta-requerimiento-contra-110-colombianos-acusados-de-lavado/85101708.

40 Interview with law enforcement, Abuja, 14 October 2025.

41 Interview with an individual involved in cybercrime, Lagos, 12 October 2025.

42 Sarfaraz Shaikh, Fake call centre busted, mastermind on run, *Ahmedabad Mirror*, 6 May 2025, https://www.ahmedabadmirror.com/fake-call-centre-busted-mastermind-

on-run/81890537.html; P Naveen, Gwalior police busted fraud call centre targeting US and UK citizens, *Times of India*, 2 April 2024, https://timesofindia.indiatimes.com/city/bhopal/gwalior-police-busted-fraud-call-center-targeting-us-and-uk-citizens/articleshow/108964052.cms.

43 T N Alagesh, Scam call centres move to remote budget hotels to avoid detection, *New Straits Times*, 1 December 2025, https://www.nst.com.my/news/regional/2025/12/1327637/scam-call-centres-move-remote-budget-hotels-avoid-detection.

44 **涉斯里兰卡网路金融诈骗案　10人落网包括4大马人 | 社会 | 東方網 馬來西亞東方日報**

45 Compound crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

46 China scam run from Isle of Man, BBC World Service, 23 August 2024, https://www.bbc.co.uk/news/articles/cz6x1ql1yelo.

47 Renting a hotel in the Taishan District to receive signals from mainland China to commit crimes, Exmoo, 26 February 2020, https://www.exmoo.com/article/142223.html; Malaysian woman suspected of setting up telecom fraud den, TDM, 17 May 2025, https://apps.tdm.com.mo/zh-hant/news-detail/1089823

48 Bernadette Carreon and Emanuel Stoakes, Foreign workers, local sponsors: Inside Palau's hotel scam centers, OCCRP, 22 December 2025, https://www.occrp.org/en/investigation/foreign-workers-local-sponsors-inside-palaus-hotel-scam-centers.

49 The horrible 5-month life in scamming compounds, Humanity Research Consultancy, 13 July 2024, https://www.humanity-consultancy.com/updates/the-horrible-5-month-life-in-scamming-compounds; Danielle Keeton-Olsen and Mech Dara, Rescue reveals scam compound at Koh Kong's UDG, VOD, 24 August 2022, https://vodenglish.news/rescue-reveals-scam-compound-at-koh-kongs-udg/.

50 FBI, foreign attachés inspect O'Smach scam hub with Thai Army, *The Nation Thailand*, 2 February 2026, https://www.nationthailand.com/news/general/40062017; Poppy McPherson and Tim Kelly, Scammers' abandoned compound exposes brutality and banality of fraud, Reuters, 6 February 2026, https://www.reuters.com/world/china/scammers-abandoned-cambodia-compound-exposes-brutality-banality-fraud-2026-02-06/.

51 Irmgard de la Cruz, *Búsqueda de personal calificado atrae cada vez más call centers a las ciudades*, Diario Libre, 24 April 2024, https://www.diariolibre.com/economia/negocios/2024/04/24/personal-calificado-atrae-a-mas-call-centers-hacia-las-ciudades/2700185.

52 Irmgard de la Cruz, *Búsqueda de personal calificado atrae cada vez más call centers a las ciudades*, Diario Libre, 24 April 2024, https://www.diariolibre.com/economia/negocios/2024/04/24/personal-calificado-atrae-a-mas-call-centers-hacia-las-ciudades/2700185; Sixteen people charged with conspiracy to defraud hundreds of elderly Americans of millions of dollars, Justice Department (USAO–D.N.J.), 30 April 2024, https://www.justice.gov/usao-nj/pr/sixteen-people-charged-conspiracy-defraud-hundreds-elderly-americans-millions-dollars; 3 Additional Dominican Nationals extradited to face 'grandparent scam' charges, ICE Newsroom, archived 9 August 2024, https://www.ice.gov/news/releases/3-additional-dominican-nationals-extradited-face-grandparent-scam-charges.

53 *Ministerio Público pone en marcha Operación Discovery 2.0 contra red del cibercrimen estafó a cientos de estadounidenses*, Press Agency of the Attorney General's Office of the Dominican Republic, 4 August 2023, https://pgr.gob.do/ministerio-publico-pone-en-marcha-operacion-discovery-2-0-contra-red-del-cibercrimen-estafo-a-cientos-de-estadounidenses/.

54 Alex Goodwin, Scammer's paradise? An assessment of scam call centres in Eurasia, GI-TOC, forthcoming.

55 Compound crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

56 Uncovering the spread of human trafficking for online fraud into Laos and Dubai, Humanity Research Consultancy (HRC), July 2024, https://cdn.prod.website-files.com/662f-5d242a3e7860ebcfde4f/66bec89de33fb0311442d888_Asia-CTIP%20Laos%20Dubai%20Investigation.pdf.

57 Ibid.

58 Jason Tower, Crossroads of competition: China in Southeast Asia and the Pacific Islands, Testimony before the USCC, China-linked transnational organized crime in Southeast Asia: A rising threat to U.S. national security, United States Institute of Peace, 20 March 2025, https://www.uscc.gov/sites/default/files/2025-03/Jason_Tower_Testimony.pdf.

59 Ibid.

60 Jason Tower and Kristina Amerhauser, Myanmar's scam economy poses growing threats to African security, News24, 3 November 2025, https://www.news24.com/southafrica/analysis-myanmars-scam-economy-poses-growing-threats-to-african-security-20251102-0925.

61 Compound Crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

62 Treasury sanctions Burma warlord and militia tied to cyber scam operations, US Department of Treasury, 5 May 2025, https://home.treasury.gov/news/press-releases/sb0129; Saw Chit Thu, European Commission, EU Sanctions Tracker, 29 October 2024, https://data.europa.eu/apps/eusanctionstracker/subjects/168264; UK and allies sanction human rights abusers, UK Government, 8 December 2023, https://www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers.

63 Matt Burgess, The Destruction of a notorious Myanmar scam compound appears to have been 'performative', Wired, 26 November 2025, https://www.wired.com/story/myanmar-kk-park-scam-compound-destruction/.

64 Diplomatic Briefing on Combating Online Scams in Cambodia, Ministry of Foreign Affairs and International Cooperation of the Kingdom of Cambodia, 20 February 2026, https://www.mfaic.gov.kh/en/media/view/2026-02-20-press-release-diplomatic-briefing-on-combating-online-scams-in-cambodia-15-40-39.

65 Jonathan Head, Casinos, high-rises and fraud: The BBC visits a bizarre city built on scams, BBC, 7 February 2025, https://www.bbc.com/news/articles/c04nx1vnw17o; Compound crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

66 Nathan Ruser, Scamland Myanmar: How conflict and crime syndicates built a global fraud industry, ASPI, 8 September 2025, https://www.aspi.org.au/report/scamland-myanmar-how-conflict-and-crime-syndicates-built-a-global-fraud-industry/.

67 Mekong Risk Monitor, Issue 1, GI-TOC, December 2025, https://globalinitiative.net/analysis/mekong-risk-monitor-1/.

68 Jason Tower and Kristina Amerhauser, The fall of a cyber scam kingpin: Will Chen Zhi's arrest and extradition be a wake-up call for scam bosses in the Mekong?, GI-TOC, 29 January 2026, https://globalinitiative.net/analysis/will-chen-zhis-arrest-and-extradition-be-a-wake-up-call-for-scam-bosses-in-the-mekong/.

69 Christine Ro, Scam compound raids in Cambodia leave trafficking survivors stranded, Forbes, 1 March 2026, https://www.forbes.com/sites/christinero/2026/03/01/scam-compound-raids-in-cambodia-leave-trafficking-survivors-stranded/; Jason Tower, Scam empire strikes back: Crackdowns on Myanmar's scam industry have had little material impact, GI-TOC, 27 August 2025, https://globalinitiative.net/analysis/scam-empire-strikes-back-crackdowns-on-myanmars-scam-industry-have-had-little-material-impact/.

70 Kristina Amerhauser and Audrey Thill, The business of exploitation: The economics of cyber scam operations in South East Asia, GI-TOC, August 2025, globalinitiative.net/analysis/cyber-scam-operations-southeast-asia/.

71 Nazarudin Latif, Indonesia deports 153 Chinese nationals accused of running online love scams, 20 September 2023, https://www.benarnews.org/english/news/indonesian/china-love-scammers-deported-09202023145154.html.

72 Over 2,000 arrested in Malaysia's anti-scam crackdown, Xinhua, 31 October 2025, https://english.news.cn/20251031/2d7caa4460a34a97817f4ce6357b3be8/c.html.

73 Southeast Asia and the Pacific Organized Crime Threat Alert, UNODC, 11 September 2025, https://www.unodc.org/roseap/en/2025/09/timor-leste-organized-crime/story.html.

74 Sri Lanka fast becoming hub for international scam operations, *The Sunday Times*, 13 October 2024, https://www.sundaytimes.lk/241013/news/sri-lanka-fast-becoming-hub-for-international-scam-operations-574106.html.

75 20 alleged Chinese scammers arrested in a raid in Chiang Mai, Thai PBS World, 31 October 2025, https://world.thaipbs.or.th/detail/59369.

76 Treasury Sanctions Corrupt Actors in Africa and Asia, US Department of Treasury, 9 December 2020, https://home.treasury.gov/news/press-releases/sm1206.

77 Rebecca Tan and Pei-Lin Wu, Chinese association accused of mixing crime and patriotism as it serves Beijing, *The Washington Post*, 24 June 2025, https://www.washingtonpost.com/world/interactive/2025/china-hongmen-organized-crime-geopolitics/.

78 Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes, United States Attorney's Office, 14 October 2025, https://www.justice.gov/usao-edny/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged.

79 Ya New and Andrew Nachemson, 'Like slaves': Myanmar workers trafficked to Laos scam hub, Frontier Myanmar, 19 June 2024, https://www.frontiermyanmar.net/en/like-slaves-myanmar- workers-trafficked-to-laos-scam-hub/; Information provided by an expert, September 2024.

80 Natalija Jovanovic, *'Sve je izgledalo kao legitimni biznis': Beograd u srcu istrage o kripto prevari*, Radio Free Europe, 2 March 2023, https://www.slobodnaevropa.org/a/beograd-u-srcu-kripto-prevare/32296388.html.

81 See, for example, Trail of broken lives leads to Kyiv call center, OCCRP, 2 March 2020, https://www.occrp.org/en/project/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center; Web of call-center scammers reaches into Albania, Georgia, OCCRP, 6 March 2020, https://www.occrp.org/en/project/fraud-factory/web-of-call-center-scammers-reaches-into-albania-georgia; James Dowsett and Graham Stack, German court sentences key figure in massive call center scam operation exposed by OCCRP, OCCRP, 27 February 2026, https://www.occrp.org/en/news/german-court-jails-key-figure-in-massive-call-center-scam-operation-exposed-by-occrp.

82 Focus group study with five financial crimes investigators, August 2025.

83 *Türkiye'ye kaçan Rus hackerlar dolandiriciliga basladi!*, Son Kale Izmir, 10 September 2023, https://www.sonkaleizmir.com/haber/Turkiye-ye-kacan-Rus-hackerlar-dolandiriciliga-basladi/138705.

84 *Hacker krizi: Rusya'dan kaçan hackerlar Türkiye'de dolandırıcılığa başladı*, Panorama News, 10 September 2023, https://

panorama-news.de/turkiye-gundemi/hacker-krizi-rusyadan-kacan-hackerlar-turkiyede-dolandiriciliga-basladi/; interview with a former police officer who worked in the Anti-Fraud Bureau, November, 2025.

85 Jason Tower, Exporting fraud. China's acquiescence to Myanmar's military regime fuels 'foreigner butchering' scam epidemic, GI-TOC, 10 October 2025, https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/.

86 INTERPOL operation strikes major blow against West African financial crime, INTERPOL, 16 July 2024, https://www.interpol.int/News-and-Events/News/2024/INTERPOL-operation-strikes-major-blow-against-West-African-financial-crime.

87 EFCC arrests four Chinese, 101 Nigerians for internet fraud, Punch, 10 January 2025, https://punchng.com/efcc-arrests-four-chinese-101-nigerians-for-suspected-internet-fraud/#google_vignette.

88 Ibid.

89 Interview with an individual involved in cybercrime, Lagos, 12 October 2025.

90 How Yahoo boys befriend, bribe policemen, soldiers to evade justice, Punch, 11 December 2021, https://punchng.com/how-yahoo-boys-befriend-bribe-policemen-soldiers-to-evade-justice/.

91 Police arrest 130 Chinese, Nigerians for alleged cybercrime in Abuja, Vanguard, 3 November 2024, https://www.vanguardngr.com/2024/11/police-arrest-130-chinese-nigerians-for-alleged-cybercrime-in-abuja/; EFCC busts cybercrime, romance fraud syndicate in Lagos, arrests scores of foreign nationals, This Day, 17 December 2024, https://www.thisdaylive.com/2024/12/17/efcc-busts-cybercrime-romance-fraud-syndicate-in-lagos-arrests-scores-of-foreign-nationals/.

92 In Georgia, for instance, the scamming of Georgians was apparently forbidden. One prominent transnational network with ties to the Georgia operation also reportedly had a rule saying scammers could not target citizens of the country where the call centre is based. Varlamov, Fraudsters: How Russians are being defrauded of billions – Prison call centers, offices in Ukraine, neural networks, the dark web, YouTube, 1 April 2025, https://www.youtube.com/watch?v=6dRA71QdSCY&t=2506s; interview with investigative journalists, Tbilisi, October 2025.

93 PBBM signs into law Anti-POGO Act of 2025, institutionalizing ban on POGOs, Office of the President of the Philippines, 29 October 2025, https://pco.gov.ph/news_releases/pbbm-signs-into-law-anti-pogo-act-of-2025-institutionalizing-ban-on-pogos/.

94 Online briefing, Jason Tower, senior expert, GI-TOC, 17 February 2026.

95 UNODC, Ukraine: Organized crime dynamics in the context of war, July 2025, https://www.unodc.org/documents/data-and-analysis/Ukraine/Ukraine_OC_Study.pdf.

96 Interview with member of parliament (Verkhovna Rada), Kyiv, February 2024.

97 For example, see Branches of illegality: Cambodia's illegal logging structures, GI-TOC, September 2022, https://globalinitiative.net/wp-content/uploads/2022/09/Cambodia-Logging-Report-web-v2.pdf.

98 Interview with police investigator of the São Paulo Civil Police fraud division, September 2025.

99 Interview with Brazilian federal police officer, September 2025.

100 Pedro S Teixera, *PCC e commando Vermelho investem em surto de golpes no Whatsapp e da falsa central telefonica, Folha de S.Paulo*, 15 December 2023, https://www1.folha.uol.com.br/mercado/2023/12/pcc-e-comando-vermelho-investem-em-surto-de-golpes-no-whatsapp-e-da-falsa-central-telefonica.shtml.

101 Interview with cybercrime researcher, September 2025.

102 Many of these types of operations have also been raided by police in Thailand, Indonesia and Malaysia.

103 Interview with the Attorney General's Office, Attorney General's Office Bunker in Bogotá, January 7, 2026.

104 Interview with a lawyer, Tbilisi, October 2025.

105 Interviews with three forensic investigators working for an international law enforcement task team dealing with West African cyberfraud syndicates, Cape Town, 18 August 2025.

106 Australian Taxation Office, accessed 18 November 2025, https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/financial-crime/boiler-room-schemes; Boiler Room Definition, How It Operates, Common Scams, Investopedia, accessed November 18, 2025, https://www.investopedia.com/terms/b/boilerroom.asp.

107 Interviews conducted with several law enforcement officers across different disciplines over years of research.

108 Interviews with three forensic investigators working for an international law enforcement task team dealing with West African cyberfraud syndicates, Cape Town, 18 August 2025.

109 Interview with senior US investigator looking into Nigerian confraternities, 24 October 2025, Cape Town.

110 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025.

111 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; interview with senior US investigator investigating Nigerian confraternities, 24 October 2025, Cape Town.

112 Ibid.

113 Ibid.

114 Ibid.; interview with forensic investigator from another major South African bank, Cape Town, 19 November 2025.

115 Interview with senior US investigator looking into Nigerian confraternities, 24 October 2025.
116 Interview with senior US investigator looking into Nigerian confraternities, Cape Town, 24 October 2025; Violent Cult That Became a Global Mafia, BBC, 13 December 2021, https://www.bbc.com/news/world-africa-59614595.
117 Kovelin Naidoo, West African organised crime groups involved in cyberfraud and the applicability of organised crime, *Criminological Theory*, MSc cybercrime degree, University of Portsmouth, Institute of Criminal Justice Studies, 2023.
118 *The Ultra-Violent Cult That Became a Global Mafia*, BBC, 13 December 2021, https://www.bbc.com/news/world-africa-59614595.
119 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; interview with senior US investigator looking into Nigerian confraternities, Cape Town, 24 October 2025.
120 Telephone interview with Gary Warner, associate professor at the University of Alabama at Birmingham and director of the Computer Forensics Research Lab, 22 October 2021.
121 Ibid.
122 Interviews with three forensic investigators working for an international law enforcement task team dealing with West African cyberfraud syndicates, Cape Town, 18 August 2025; interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; crackdown on alleged internet scammer group Black Axe, *Sunday Times*, 23 October 2021, https://www.sundaytimes.timeslive.co.za/sunday-times/news/2021-10-24-crackdown-on-alleged-internet-scammer-group-black-axe/.
123 Information presented at the Interpol CyberEx meeting in Hong Kong, 2–3 February 2026; see also Compound crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.
124 Position paper on caller ID spoofing, Europol, 27 October 2025, https://www.europol.europa.eu/publications-events/publications/position-paper-caller-id-spoofing.
125 *Ausgewählte Zahlen im Überblick*, Bundesministerium des Innern und für Heimat, 2024 Polizeiliche Kriminalstatistik, p. 28, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2024/FachlicheBroschueren/IMK-Bericht.pdf?__blob=publicationFile&v=13.
126 *Ministerio Público despliega la Operación Discovery 2.0 contra el cibercrimen internacional*, Diario Libre, 4 August 2025, https://www.diariolibre.com/actualidad/justicia/2023/08/04/desarticulan-red-de-cibercrimen-en-operacion-discovery-20/2423619.
127 Poppy McPherson, Ally J Levine and Han Huang, A scammer's blueprint. How cybercriminals plot to rob a target within a week, Reuters, 8 January 2026, https://www.reuters.com/graphics/SOUTHEASTASIA-SCAMS/MANUALS/klpyjlqelvg/.
128 *Ministerio Público despliega la Operación Discovery 2.0 contra el cibercrimen internacional*, Diario Libre, 4 August 2025, https://www.diariolibre.com/actualidad/justicia/2023/08/04/desarticulan-red-de-cibercrimen-en-operacion-discovery-20/2423619.
129 Vendor listing on Dark Net Army marketplace, observed during primary OSINT collection by GI-TOC's Europe Observatory, October 2025.
130 Vendor 'Gold Apple' is a well-known seller of data, as well as other digital products like malware. Observation on the Torzon dark web marketplace, accessed via Tor, October 2025.
131 Observation on the nexus dark web marketplace, accessed via Tor, October 2025.
132 Observation on dread, online marketplace, accessed via Tor, October 2025.
133 Interview with fraud experts in Germany, October 2025.
134 Focus group study with five financial crimes investigators, August 2025.
135 Compound Crime: Cyber scam operations in South East Asia, GI-TOC, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.
136 Dennis Schirrmacher, *40.000 SIM-Karten konfisziert: Europol sprengt Betrügerring*, Heise Online, 20 October 2025, https://www.heise.de/news/40-000-SIM-Karten-konfisziert-Europol-sprengt-SIMCARTEL-Betruegerring-10784925.html#; Cybercrime-as-a-service takedown: 7 arrested, Europol, 17 October 2025, https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested.
137 Jonathan Head and Rachel Hagan, SpaceX says it has cut Starlink services to Myanmar scam camps, BBC, 22 October 2025, https://www.bbc.co.uk/news/articles/cpd2e5541d1o.
138 Hanna Park, How a guilt-ridden cyberscammer escaped his Cambodian compound – and teamed up with the people it ruined, CNN, 26 January 2026, https://edition.cnn.com/2026/01/26/asia/south-korean-victims-southeast-asia-scam-network-intl-hnk-dst.
139 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; Interview with senior US investigator looking into Nigerian confraternities, Cape Town, 24 October 2025.
140 Interview with a woman involved in cybercrime in Jos, 23 October 2025.
141 Ibid.
142 Ibid.

143 Lindsey Kennedy and Nathan Paul Southern, Minimizing risks of criminal exposure to scam compounds in corporate supply chains: A guide for real estate investors, developers and construction contractors, GI-TOC, December 2025, https://globalinitiative.net/wp-content/uploads/2025/12/Lindsey-Kennedy-Nathan-Paul-Southern-Minimizing-risks-of-criminal-exposure-to-scam-compounds-in-corporate-supply-chains-GI-TOC-December-2025.pdf.

144 Lindsey Kennedy and Nathan Paul Southern, Minimizing risks of criminal exposure to scam compounds in corporate supply chains: A guide for suppliers and partners, GI-TOC, January 2026, https://globalinitiative.net/wp-content/uploads/2025/12/Lindsey-Kennedy-Nathan-Paul-Southern-Minimizing-risks-of-criminal-exposure-to-scam-compounds-in-corporate-supply-chains-A-guide-for-suppliers-and--partners-GI-TOC-January-2026.pdf.

145 USIP Senior Study Group, Transnational crime in Southeast Asia: A growing threat to global peace and security, USIP, May 2024, https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.

146 Meaning if the money is already stolen in crypto, there is no need to convert it. For example, grandparent scams in the Dominican Republic remain cash-heavy (it is collected by courier), while romance and investment scams are more often linked to cryptocurrencies and OTC brokers.

147 Israel Ojoko, EFCC uncovers use of cryptocurrency in illegal arms importation into Nigeria, Nairametrics, 27 February 2025, https://nairametrics.com/2025/02/27/efcc-uncovers-use-of-cryptocurrency-in-illegal-arms-importation-into-nigeria/.

148 Statement by a law enforcement liaison officer at the CyberCrime EX Meeting, Hong Kong, 2-3 February 2026.

149 Kristina Amerhauser and Audrey Thill, The business of exploitation: The economics of cyber scam operations in Southeast Asia, GI-TOC, August 2025, https://globalinitiative.net/analysis/cyber-scam-operations-southeast-asia/.

150 USDT and TRON are the main cryptocurrencies utilized by Brazilian and South East Asian fraudsters – no information available on other scam markets. See Kristina Amerhauser and Audrey Thill, The business of exploitation: The economics of cyber scam operations in South East Asia, GI-TOC, August 2025, https://globalinitiative.net/analysis/cyber-scam-operations-southeast-asia/; GI-TOC interview with cybercrime researcher, September 2025.

151 Kristina Amerhauser and Audrey Thill, The business of exploitation: The economics of cyber scam operations in South East Asia, GI-TOC, August 2025, https://globalinitiative.net/analysis/cyber-scam-operations-southeast-asia/.

152 OSINT collection observation of payment instructions across multiple dark web vendor listings, October 2025.

153 Sixteen People Charged with Conspiracy to Defraud Hundreds of Elderly Americans of Millions of Dollars, Justice Department (USAO–D.N.J.), 30 April 2024, https://www.justice.gov/usao-nj/pr/sixteen-people-charged-conspiracy-defraud-hundreds-elderly-americans-millions-dollars; US Immigration and Customs Enforcement, 3 Additional Dominican Nationals Extradited to Face 'Grandparent Scam' Charges, ICE Newsroom, 9 August 2024, https://www.ice.gov/news/releases/3-additional-dominican-nationals-extradited-face-grandparent-scam-charges.

154 *Ministerio Público despliega la Operación Discovery 2.0 contra el cibercrimen internacional*, Diario Libre, 4 August 2025, https://www.diariolibre.com/actualidad/justicia/2023/08/04/desarticulan-red-de-cibercrimen-en-operacion-discovery-20/2423619.

155 Interview with individual involved in cybercrime in Abuja, 14 October 2025.

156 Interviews conducted with fraud experts in Germany, October 2025; Ebru Erkan, Counting the costs, Türkiye is taking steps to contain rising cases of fraud. Will they be effective?, GI-TOC, 14 January 2025, https://globalinitiative.net/analysis/turkiye-to-contain-fraud-will-they-be-effective/.

157 Observation on Facebook, accessed October 2025.

158 Alex Goodwin, Scammer's paradise? An assessment of scam call centres in Eurasia, GI-TOC, forthcoming.

159 *Fiscalía ordena captura de estructura de colombianos que utilizaban a salvadoreños como mulas financieras para lavar dinero proveniente estafas y hurtos informáticos, entre otras actividades ilícitas*, Fiscalía General de la República (FGR), El Salvador, 18 July 2024, https://www.fiscalia.gob.sv/fiscalia-ordena-captura-de-estructura-de-colombianos-que-utilizaban-a-salvadorenos-como-mulas-financieras-para-lavar-dinero-proveniente-estafas-y-hurtos-informaticos-entre-otras-actividades-ilicitas/.

160 Interview with police investigator of the São Paulo Civil Police fraud division in September 2025, Mekong Risk Monitor, Issue 2, GI-TOC, forthcoming.

161 A young man who rented out his bank account for 8,000 Turkish Lira experienced a nightmare, Haberler, 1 June 2025, https://www.haberler.com/guncel/8-bin-lira-karsiliginda-hesabini-kullandiran-genc-dolandiriciliktan-tutuklandi-18697065-haberi/.

162 Money-mule ring busted: four suspects arrested, including bank employee who opened accounts for 500 baht each, Khaosod Online, 17 January 2026, https://www.khaosod.co.th/special-stories/news_10101502.

163 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; interview with senior US investigator looking into Nigerian confraternities, Cape Town, 24 October 2025; interviews with three forensic investigators working for an international law enforcement task team dealing with West African cyberfraud syndicates, Cape Town, 18 August 2025' Mekong Risk Monitor, Issue 2, GI-TOC, forthcoming.

164 Mekong Risk Monitor, Issue 2, GI-TOC, forthcoming.

165 More than 24 million Brazilians engaged in online betting in 2024, with a monthly average of BRL20.8 billion (USD4 billion) spent in this market domestically. Criminal operatives involved in the fraud trade go on to utilize these laundered funds to invest in luxury real estate and high-end vehicles. See *A metamorfose digital: como as facções brasileiras estão trocando o fuzil pelo phishing*, Fonte Segura, 18 June 2025, https://fontesegura.forumseguranca.org.br/a-metamorfose-digital-como-as-faccoes-brasileiras-estao-trocando-o-fuzil-pelo-phishing/3; João Batista Jr and Alessandra Medina, *Como as bets produziram a pandemia do vício*, Piauí, 3 January 2025, https://piaui.folha.uol.com.br/como-as-bets-produziram-a-pandemia-do-vicio/; Mauricio Savarese and Lucas Dumphreys, As sports betting addiction takes hold in Brazil, the government moves to crack down, AP, 8 November 2024, https://apnews.com/article/sports-betting-brazil-crisis-e199e0ef30228c15fd25820b1a69a900.

166 Interview with senior law enforcement official, Islamabad, 11 July 2025.

167 Interviews with casino industry workers, Colombo, 3 February 2026.

168 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; interview with senior US investigator looking into Nigerian confraternities, Cape Town, 24 October 2025; interviews with three forensic investigators working for an international law enforcement task team dealing with West African cyberfraud syndicates, Cape Town, 18 August 2025.

169 Kristina Amerhauser and Audrey Thill, The business of exploitation: The economics of cyber scam operations in Southeast Asia, GI-TOC, August 2025, https://globalinitiative.net/analysis/cyber-scam-operations-southeast-asia/.

170 Internet Crime Report 2024, Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf; FinCEN Finds Cambodia-based Huione *Group to Be of Primary Money Laundering Concern*, *Proposes a Rule to Combat Cyber Scams and Heists*, U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) press release, 1 May 2025, https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern; National Money Laundering Risk Assessment 2024, U.S. Department of the Treasury, February 2024, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

171 Lindsey Kennedy and Nathan Paul Southern, Where does North Korea get its cash?: How the scam industry created new money laundering avenues for North Korea, GI-TOC, 31 March 2025, https://globalinitiative.net/analysis/where-does-north-korea-get-its-cash/.

172 Interview with Brazilian federal police officer, September 2025.

173 Interview with individual involved in cybercrime in Lagos, 12 October 2025.

174 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; interview with senior US investigator looking into Nigerian confraternities, Cape Town, 24 October 2025.

175 Interview with forensic investigator from a major South African bank involved in law enforcement investigations into Nigerian confraternities, 24 October 2025; interview with senior US investigator looking into Nigerian confraternities, Cape Town, 24 October 2025; see Aron Hyman, Sandton fraud kingpin had biometric information deleted from prison, TimesLIVE, 2 September 2022, https://www.timeslive.co.za/news/south-africa/2022-09-02-sandton-fraud-kingpin-had-biometric-information-deleted-from-prison/.

176 Compound crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

177 Afeer Hanafi, How Yahoo boys befriend, bribe policemen, soldiers to evade justice, Punch, 11 December 2021, https://punchng.com/how-yahoo-boys-befriend-bribe-policemen-soldiers-to-evade-justice/.

178 Interview with a member of parliament, Kyiv, February 2025.

179 In an interview in Kyiv in February 2025, a member of parliament said: 'We received docs showing the numbers and the recipients in law enforcement (US$10 000–15 000 a month). We had information about call centres contacting all law enforcement agencies.' In another media report, the figure of US$12 000 a month was mentioned. See: Olga Paliy, Thousands of 'employees', bribes, crypto and torture: how fraudulent call centres in Ukraine are organized, Informator, 26 July 2023, https://informator.ua/uk/tisyachi-spivrobitnikivhabari-kripta-ta-torturi-yak-vlashtovani-shahrayski-kol-centri-vukrajini.

180 Assessment conducted by C-Análisis, February 2025, unpublished, drawing on interviews with former inmates of La Modelo and La Picota, Bogotá, 30 December 2025.

181 Compound crime: Cyber scam operations in South East Asia, GI-TOC, May 2025, https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

182 Treasury Sanctions Cambodian Tycoon and Business Linked to Human Trafficking and Forced Labor in Furtherance of Cyber and Virtual Currency Scams, US Treasury Department, 12 September 2024, https://home.treasury.gov/news/press-releases/jy2576.

183 Jason Tower and Kristina Amerhauser, The fall of a cyber scam kingpin: Will Chen Zhi's arrest and extradition be a wake-up call for scam bosses in the Mekong?, GI-TOC,

29 January 2026, https://globalinitiative.net/analysis/will-chen-zhis-arrest-and-extradition-be-a-wake-up-call-for-scam-bosses-in-the-mekong/.

184 Myanmar junta's anti-scam czar purged in bribery scandal, The Irrawaddy, 12 February 2026, https://www.irrawaddy.com/news/burma/myanmar-juntas-anti-scam-czar-purged-in-bribery-scandal.html.

185 Compound crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

186 Interview with a former police officer who worked in the Anti-Fraud Bureau, August, 2025.

187 Mahmut Cengiz and Kutluer Karademir, The impacts of authoritarianism on organized crime in Turkey, *Small Wars Journal*, 11 August 2020, https://archive.smallwarsjournal.com/jrnl/art/impacts-authoritarianism-organized-crime-turkey.

188 Ibid.

189 Ebru Erkan, Counting the costs: Türkiye is taking steps to contain rising cases of fraud. Will they be effective?, GI-TOC, 14 January 2025, https://globalinitiative.net/analysis/turkiye-to-contain-fraud-will-they-be-effective/.

190 Web of call-center scammers reaches into Albania, Georgia, OCCRP, 6 March 2020, https://www.occrp.org/en/project/fraud-factory/web-of-call-center-scammers-reaches-into-albania-georgia.

191 საქართველო ს პროკურატურამ … გახსნა, Prosecutor's Office of Georgia, 6 September 2024, https://pog.gov.ge/news/saqarTvelos-prokuraturam-germaniis-federaciuli-respublikis-samarTaldamcavebTan-TanamshromlobiT-qol.

192 Verdict of Tbilisi City Court, unpublished official document, 27 June 2025.

193 Interview with NGO, June 2025.

194 Interviews with investigative journalists, a lawyer and a diplomat, Tbilisi, October 2025; interview with NGO, June 2025.

195 Interview with Georgian cyber security expert, December 2025.

196 Interview with diplomat, Tbilisi, October 2025.

197 Rayhan Demytrie, Spectacular downfall of Georgia's ex-PM accused of having $6.5m in his flat, BBC, 24 October 2025, https://www.bbc.com/news/articles/cjekw5jxw89o; Ex-Prime Minister Garibashvili to serve five years in prison after plea deal, Civil.ge, 12 January 2026, https://civil.ge/archives/717027.

198 OCCRP, Georgia detains ex-security chief over alleged bribes tied to global scam call centers, 23 December 2025, https://www.occrp.org/en/news/georgia-detains-ex-security-chief-over-alleged-bribes-tied-to-global-scam-call-centers.

199 Salome Chaduneli, Susi's boss, prosecutor general, murder contractor, journalist and swindler in one scheme – the 'call center' case, Radio Liberty, 18 February 2026, https://www.radiotavisupleba.ge/a.

200 Detained journalist Eliso Kiladze denies charges in 'call center' case, Georgia Today, 19 February 2026, https://georgiatoday.ge/detained-journalist-eliso-kiladze-denies-charges-in-call-center-case/.

201 Interview with cybercrime researcher, September 2025.

202 Layboard advert, Sales Manager, https://layboard.com/vakansiya/1546151/salesmanager.

203 Emily Fishbein and Peter Guest, Inside a romance scam compound – and how people get tricked into being there, Pulitzer Center, 27 March 2025, https://pulitzercenter.org/stories/inside-romance-scam-compound-and-how-people-get-tricked-being-there; Indulekha Aravind and ET Bureau, The man who escaped the scam rings of Cambodia, *The Economic Times*, 2 June 2024, https://economictimes.indiatimes.com/jobs/mid-career/the-man-who-escaped-the-scam-rings-of-cambodia/articleshow/110626511.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst; Vincent MacIsaac, Myanmar's scam hells can't release their captives, Irrawaddy, 6 September 2024, https://www.irrawaddy.com/news/burma/myanmars-scam-hells-cant-release-their-captives.html; Scam City: How the coup brought Shwe Kokko back to life, Frontier, 23 June 2022, https://www.frontiermyanmar.net/en/scam-city-how-the-coup-brought-shwe-kokko-back-to-life/.

204 "A wicked problem": Seeking human rights-based solutions to trafficking into cyber scam operations in South East Asia, OHCHR, 2026, https://www.ohchr.org/sites/default/files/documents/issues/trafficking/report-a-wicked-problem.pdf.

205 Based on GI-TOC's own estimate.

206 Existing research has shown that in South East Asia many people who conduct scams fall along a spectrum of exploitation. They include people trafficked for the purpose of forced criminality and they include lower-level criminals that enter this business willingly and know they are conducting scams. In addition, there is a grey zone of those that may enter voluntarily but later try to leave and cannot; those that were initially trafficked but are 'successful' at their work and decide to stay; and sometimes people who get rescued and repatriated home and then return. While this challenges the idea of a perfect victim, it is important to underline that most people continue to be exposed to significant stress and torture if they underperform. See Compound crime: Cyber scam operations in Southeast Asia, GI-TOC, May 2025, https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

207 Ibid.

208 "A wicked problem": Seeking human rights-based solutions to trafficking into cyber scam operations in South East Asia, OHCHR, 2026, https://www.ohchr.org/sites/default/files/documents/issues/trafficking/report-a-wicked-problem.pdf.

209 Interview with EOCO official, 11 September 2025; Nigerians trafficked to Ghana and forced to work as cyber-criminals for ruthless gangs, Action Aid, 27 July 2023, https://actionaid.org/stories/2023/nigerians-trafficked-ghana-and-forced-work-cyber-criminals-ruthless-gangs.

210 219 rescued from human trafficking and cybercrime ring in Ghana, Africa News, 18 April 2025, https://www.africanews.com/2025/04/18/219-rescued-from-human-trafficking-and-cybercrime-ring-in-ghana/.

211 Interview with senior law enforcement official, Islamabad, 11 July 2025.

212 Uncovering the spread of human trafficking for online fraud into Laos and Dubai, Humanity Research Consultancy (HRC), July 2024, https://cdn.prod.website-files.com/662f-5d242a3e7860ebcfde4f/66bec89de33fb0311442d888_Asia-CTIP%20Laos%20Dubai%20Investigation.pdf.

213 Interview with Nepal law enforcement, February 4, 2026; interview with Sri Lanka Ministry of Foreign Affairs, February 2, 2026.

214 Interviews with former scammers A and L, Ukraine, February 2025.

215 Interview with an individual involved in cybercrime, Abuja, 14 October 2025.

216 Interviews with former scammers A and L, Ukraine, February 2025.

217 Tuesday Reitano and Mark Shaw, *Criminal Contagion: How Mafias, Gangsters and Scammers Profit from a Pandemic*, C. Hurst & Co, 2021; Criminals exploit Covid-19 pandemic with rise in scams targeting victims online, UK Finance, no date, https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online; Sun Yaohui, Beware of new overseas scams during the pandemic, People.cn, 23 July 2020, http://legal.people.com.cn/n1/2020/0723/c42510-31794877.html

218 Interview with member of parliament, Kyiv, February 2025; Jack Meegan-Vickers, Scam call centres in Ukraine, 21 October 2023, https://globalinitiative.net/analysis/scam-call-centres-in-ukraine/.

219 Dwaipayan Ghosh, Fraud calls from Pakistan numbers rise amid new malware threat, *Times of India*, 13 May 2025, https://timesofindia.indiatimes.com/city/kolkata/fraud-calls-from-pakistan-numbers-rise-amid-new-malware-threat/articleshow/121143100.cms.

220 Jason G Tower, Exporting fraud: China's acquiescence to Myanmar's military regime fuels 'foreigner butchering' scam epidemic, GI-TOC, 10 October 2025, https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/.

221 For example, China has tacitly backed an offensive by an ethnic insurgent alliance in Shan State in late 2023. China has put on trial and sentenced to death several clan members linked to running scam centres in the area. See Koh Ewe and Jonathan Head, China executes 11 members of Myanmar scam mafia, BBC, 29 January 2026, https://www.bbc.com/news/articles/cx2gdrvy9gjo.

222 On Russia, Belarus, Kazakhstan and Uzbekistan cooperation, see The situation was turned around. For the first time in recent years, the Ministry of Internal Affairs records a decrease in cybercrime, BelTA, 5 November 2025, https://belta.by/society/view/situatsiju-udalos-perelomit-mvd-vpervye-za-poslednie-gody-fiksiruet-snizhenie-kiberprestuplenij-747107-2025/; Law enforcement officers of Belarus and Russia have planned joint steps to suppress cybercrime, BelTA, 21 November 2025, https://belta.by/society/view/pravoohraniteli-belarusi-i-rossii-splanirovali-sovmestnye-shagi-po-presecheniju-kiberprestuplenij-750117-2025; On Kyrgyzstan cooperation, see A citizen of Belarus suspected of major fraud was detained in Bishkek, Banks, 6 June 2024, https://banks.kg/news/citizen-belarus-suspected-major-fraud.

223 For example, see the case of She Zhijiang who claimed to be a Chinese spy, asked for extradition to Cambodia and other countries to avoid extradition to China. See Poppy McPherson and Panu Wongcha-um, Detained tycoon She Zhijiang, who says he spied for China, alleges abuse in Thai jail, Reuters, 26 January 2025, https://www.reuters.com/world/asia-pacific/gambling-tycoon-abused-thai-jail-after-saying-he-spied-china-lawyers-say-2025-01-24/.

224 EIU's 2024 Democracy Index: trend of global democratic decline and strengthening authoritarianism continues through 2024, Economist Intelligence Unit, 27 February 2025, https://www.eiu.com/n/democracy-index-2024/.

225 Iskra Kirova, Foreign agent laws in the authoritarian playbook, Human Rights Watch, 19 September 2024, https://www.hrw.org/news/2024/09/19/foreign-agent-laws-authoritarian-playbook#:~:text=From%20Russia%20to%20Kyrgyzstan%2C%20and,NGOs%20in%20Moscow%2C%20including%20Memorial.

226 Compound crime: Cyber scam operations in South East Asia, GI-TOC, May 2025, https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf; Meeting with representatives of UN agencies in Cambodia, October 2025.

227 Gemma Davies and Helena Farrand Carrapico, UK-EU Law Enforcement And Judicial Cooperation In Criminal Matters Under Part Three Of The Trade And Cooperation Agreement: The Impact on Scotland, Scottish Parliament Academic Fellowship Report, September 2024, https://www.parliament.scot/-/media/files/committees/criminal-justice-committee/research-report-on-the-impact-of-the-uks-exit-from-membership-of-the-eu-on-law-enforcement-and-judic.pdf.

228 Fuelling the future, poisoning the present: Myanmar's rare earth boom, Global Witness, 23 May 2024, https://www.globalwitness.org/en/campaigns/natural-resource-governance/fuelling-the-future-poisoning-the-present-

myanmars-rare-earth-boom/; Prem Mahadevan, Myanmar's illicit timber: Flows, drivers and actors, GI-TOC, October 2021, https://globalinitiative.net/wp-content/uploads/2021/10/Myanmars-illicit-timber-Flows-drivers-and-actors.pdf; Organised Chaos: The illicit overland timber trade between Myanmar and China, EIA, September 2015, https://eia-international.org/wp-content/uploads/EIA-Organised-Chaos-FINAL-lr1.pdf.

229 Martin Thorley, A changing landscape: China's new model of global governance and its impact on the fight against organized crime, GI-TOC, 9 May 2024, https://globalinitiative.net/analysis/china-new-model-of-global-governance-and-its-impact-on-the-fight-against-organized-crime/; Golden Triangle: How crypto scammers found a criminal paradise in Laos, Bloomberg, 19 August 2024, https://bloomberg.com/features/2024-golden-triangle-special-economic-zone/; Jason Tower and Priscilla A. Clapp, Myanmar scam hubs revive fast after China eases pressure on junta, US Institute of Peace, 26 September 2024, https://www.usip.org/publications/2024/09/myanmar-scam-hubs-revive-fast-after-china-eases-pressure-junta.

230 Jason G Tower and Kristina Amerhauser, The fall of a cyber scam kingpin: Will Chen Zhi's arrest and extradition be a wake-up call for scam bosses in the Mekong?, GI-TOC, 29 January 2026, https://globalinitiative.net/analysis/will-chen-zhis-arrest-and-extradition-be-a-wake-up-call-for-scam-bosses-in-the-mekong/.

231 Karishma Vyas, On the Myanmar-Thailand border, bombing a scam centre could barely dent the industry, ABC, 10 November 2025, https://www.abc.net.au/news/2025-11-10/myanmar-scam-centre-crackdown-on-border-with-thailand/105983376.

232 Ibid.

233 Ibid.

234 Feds seize record-breaking $15 billion in Bitcoin from alleged scam empire, Wired, 14 October 2025, https://www.wired.com/story/feds-seize-record-breaking-15-billion-in-bitcoin-from-alleged-scam-empire/.

235 Major law changes to protect people from scam adverts online, UK Government, press release, 8 March 2022, https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online.

236 Sam Rogers, International scammers steal over $1 trillion in 12 months in Global State of Scams Report 2024, GASA, 7 November 2024, https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai.

237 See https://www.globalsignalexchange.org.

238 Jason Tower, Exporting fraud: China's acquiescence to Myanmar's military regime fuels 'foreigner butchering' scam epidemic, GI-TOC, 10 October 2025, https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/.

239 Interview, New Delhi, December 2025.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net