TRANSPARENCY INTERNATIONAL
the global coalition against corruption

Anti-Corruption Helpdesk Answer

The role of corruption in scam centres

Author(s): Sam Parrett-Jung, tihelpdesk@transparency.org
Reviewer(s): Jamie Bergin, Franziska Schlichting
Date: 18 August 2026

Scam centres have emerged as a sophisticated and widespread form of cybercrime in recent years, targeting victims on a global scale. The proliferation of the scam industry is a significant governance and human rights issue enabled by corruption. The paper finds that large-scale scam operations often depend on some form of official complicity or facilitation. Such arrangements give criminals the operational protection and freedom needed to recruit, move and exploit victims of human trafficking, as well as to receive information about potential crackdowns, escape accountability or, in some cases, control scam operations in collusion with, or under the direction of, high-level government officials. Corruption-enabled scam operations are sustained by a number of enabling factors, such as weak governance and regulatory gaps. Responses therefore need to address the conditions that allow corruption in scam operations to take root, including poor oversight of high-risk border areas and special economic zones (SEZs), weak or absent anti-corruption legislation or limited cross-border cooperation.

This paper is financed by the Swedish Postcode Lottery Foundation.

SVENSKA POSTKODLOTTERIETS STIFTELSE

Query

What is the role of the role of corruption in scam centres and compounds linked to transnational organised criminal groups?

Main points

- Scam centres vary significantly in their operations and physical makeup, ranging from small apartment based operations to large compounds with defined organisational structures. Despite this, they all share similar functional components, such as a physical site, a workforce, management structures, access to digital tools and some form of local protection or enabling environment. This, coupled with their low infrastructure requirements and ability to relocate, makes them highly replicable across jurisdictions, and has contributed to proliferation in recent years.

- Corruption is generally a core enabler of scam centre operations. Bribery, political protection, official control and law enforcement collusion create a criminal ecosystem free from legal or regulatory interference.

- In Myanmar, evidence has been found that the Karen Border Guard Force, which is connected to the Myanmar military, controls and provides security to scam compounds in exchange for a cut of the profits.

- In Georgia, allegations against senior officials and politically connected actors illustrate how scam centres can become embedded in state-linked protection networks, with corrupt actors reportedly shielding operations in exchange for kickbacks.

- In Cambodia, scam operations are reportedly housed in hotels, resorts, casinos and office parks connected to political elites, while wider kleptocratic and patronage networks help protect and enable the scam economy.

- Corruption in scam operations is enabled by long-standing and embedded relationships between organised crime groups and state officials, which are sustained by recurring and self-reinforcing patronage and rent-sharing arrangements

- Scam centres are also sites of serious human rights abuse. Many workers are migrants deceived through fraudulent job offers, then subjected to forced labour, debt bondage, violence, surveillance and restrictions on movement.

- Corruption facilitates human trafficking linked to scam centres at multiple stages, such as during the recruitment stage, at border crossings and in detention centres post-escape. Therefore, anti-trafficking responses must address public sector complicity and facilitation.

- Weak governance, regulatory gaps, limited oversight of border areas and special economic zones (SEZs), conflict affected areas or areas with contested authority, poor inter-agency coordination and weak cross-border cooperation create the conditions for corruption to take root in scam operations. Therefore, responses must focus on these enabling conditions.

Contents

Introduction

Scam centres are recognised as one of the most commercially sophisticated and lucrative forms of organised crime in recent times (Amerhauser and Goodwin 2026; GI-TOC 2026). According to one estimate, the scam industry stole over US$1 trillion in 2024 alone, almost 1% of global GDP (Amerhauser and Goodwin 2026; GI-TOC 2026). The growth of this criminal industry is fuelled by the technical expansion and accessible nature of information and communications technology enabling scammers to target victims on a global scale (GI-TOC 2026). Scammers often combine approaches to deceive their victims, including through traditional romance, investment or impersonation scams, or more recently with new variations, such as digital kidnaps, malware scams or online sextortion (SEAPPI 2025).

Scam centres have been established around the world and take many forms, from individuals working in apartment rooms to large-scale, sophisticated operations located in office buildings or compounds (GI-TOC 2025; 2026). A scam operation may appear outwardly legitimate or operate within an otherwise legitimate business, blurring the lines between the legal and illegal (GI-TOC 2026). Locations in which scam centres have prospered are typically marked by limited human and technical resources, poor inter-agency coordination, weak channels for international cooperation and inadequate intelligence sharing capabilities to deal with the pervasiveness of organised crime (UNODC 2025a).

Scam centres are typically established, owned, hosted or protected by a combination of: transnational organised crime networks (UNODC 2025a); legal entities, such as casinos or hotels (Grieg 2026); politically connected local business elites (Luoluo 2025); and, in Myanmar particularly, armed groups or state-linked militias (Justice for Myanmar 2025). Organised crime groups often establish and run scam centres themselves (Armerhauser and Goodwin 2026; UNODC 2025a), but reports indicate they may also externally facilitate scam operations, such as by trafficking victims to carry out operations (OHCHR 2023; 2026). Commercial entities often provide the premises and outward appearance of lawful business activity (Amerhauser and Goodwin 2026; Greig 2026), while politically connected business elites can help embed scam centres within local economies by leasing land or property, or shielding sites from law enforcement (US DoT 2024; Sims 2024). In Myanmar, contested sovereignty and territorial control gives armed groups and state-linked militias the means to provide security and protection from state intervention (Bayer et al. 2024; Justice for Myanmar 2025).

Individuals that work in scam centres are primarily migrants in vulnerable situations, and are often victims of forced labour and human trafficking (Amnesty International 2025; OHCHR 2023; 2026; OSCE 2026). This is a growing issue, especially in Southeast

Asia, where scam compounds have become sites of systematic human trafficking, forced criminality and other severe human rights abuses (OHCHR 2023; 2026).

UNODC (2025a; b) states that corruption is a core driver facilitating the expansion and endurance of the industry. This is often underpinned by legislative and regulatory gaps in anti-corruption frameworks that create loopholes for criminal actors to exploit, or by weak governance, where criminal enterprises can undertake their activities with minimal scrutiny (UNODC 2025b). Corruption risks are also attributed to low-paid law enforcement officers and immigration officers vulnerable to bribery, as well as high-level officials such as prosecutors, government officials and judges willing to accept bribes or receive a cut of profits in return for complicity, facilitation or dismissal of charges and reduced sentences (Amerhauser and Goodwin 2026; Keeton-Olsen 2022; Luoluo 2025; OCCRP 2025; US Department of the Treasury 2024).

It is important to note that trafficking in persons for forced labour in scam centres is also enabled by corruption. Much like the operation of scam centres, corruption within law enforcement, border control and other government institutions enables criminal networks to recruit, move, detain and exploit victims (Amnesty International 2025; GI-TOC 2026; OHCHR 2023; 2026).

Scam centres

There is no single definition of a scam centre, rather a definition is applied according to the context in which it is examined, as well as the operations housed within them. Amerhauser and Goodwin (2026: 1) examine the scam centre as a "distinct organisational unit" and UNODC (2025a: 31) define a scam centre as an organised operation that steals money or information through deception. Amnesty International (2025), GI-TOC (2025) and OHCHR (2023; 2026) on the other hand, define scam centres primarily as walled-off compounds, like those typical of Southeast Asia. Scam centres in Georgia, however, are primarily defined as call centres, though the underlying logic in their operations are akin to those in other jurisdictions, including a workforce, management structures and the use of digital tools to defraud victims (Amerhauser and Goodwin 2026).

They may, however, vary considerably in their physical makeup, organisational functions and economic models (GI-TOC 2026; UNODC 2025a). Prisons have long been used as sites for scamming operations, as have apartments, houses, hotels, casinos and office spaces. These are all locations that provide greater cover and the ability to relocate with ease. Larger scam operations may be housed in extensive office spaces, follow a defined hierarchy and have dedicated departments to manage the varying functions of the operation (Amerhauser and Goodwin 2026). The clearest extreme is the scam centres found in Southeast Asia, typically understood as large walled-off compounds which have the capacity to house tens of thousands of workers (OSCE 2026; SEAPPI 2025). For example, a scam centre in Cambodia know as #8 Park reportedly has the capacity to accommodate 20,000 trafficked workers (Tabahriti 2026). Such operations often require high levels of political protection (Amerhauser and Goodwin 2026).

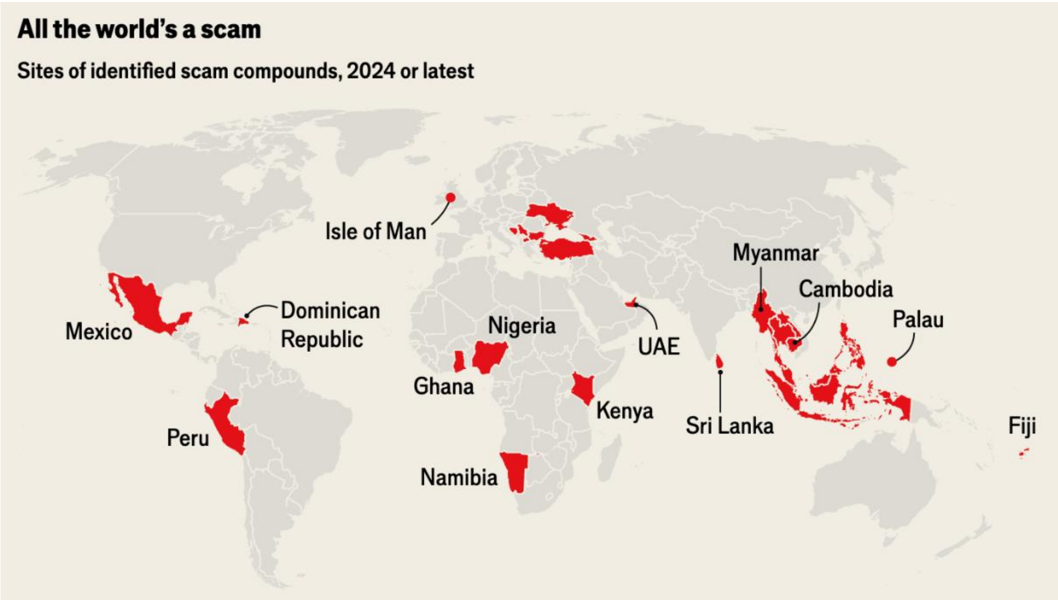
Types of scam centres

Prison scam centres operate with a captive workforce and close collusion between criminal actors and officials. They have limits to their reach due to restricted access to technology, a smaller labour pool and fewer opportunities to expand (Amerhauser and Goodwin 2026). Prison centres have been found in Russia, Ukraine, South Africa and Colombia, among other countries. Scams undertaken in these operations are relatively simple, relying on phone calls using numbers supplied to the workers. The basic nature of these operations also stems from the workforce, which is constrained to the prison demographic, typically resulting in fewer specialised skills.

In some countries, apartments, houses and small office spaces are used to house scam operations. The size of these locations means operations are less likely to attract unwanted attention from law enforcement, although reports indicate that some operations require structured arrangements with local officials (Amerhauser and Goodwin 2026).

Large-scale office spaces and compounds provide the capacity and technical facilities for high-level operations with large labour forces, resulting in significant reach (GI-TOC 2026; UNODC 2025b). These operations have a range of forms and may resemble legal call centres, with dedicated departments spanning IT, finance, HR and security (GI-TOC 2026). A single building could house licit and illicit operations on different floors, allowing criminal activity to blend into an outwardly legitimate commercial setting. The Economist (2025) identified compounds in many locations around the world:

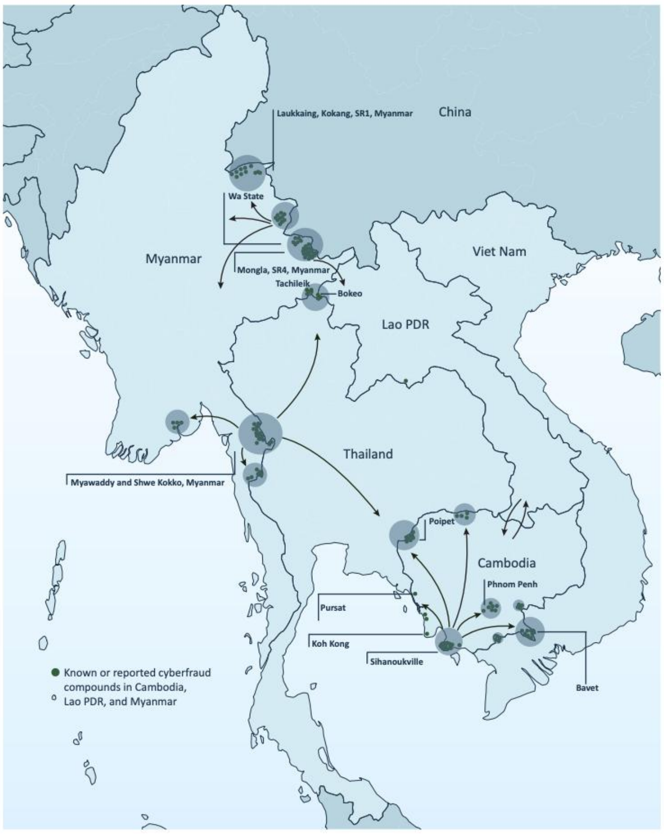
Figure 1: Global map of scam compounds identified by the Economist, 2024 or latest



Source: The Economist (2025)

The large-scale scam centre model has arguably reached its most acute form in Southeast Asia, with walled perimeters, a large, trafficked labour force and coercive or violent operational practices (O'Bryan 2025; OSCE 2026; UNODC 2025b). As these criminal operations attract significant law enforcement attention, they are often established in areas of grey governance, such as border areas, special economic zones (SEZs) or conflict affected areas, which are characterised by weak governance, regulatory gaps and opportunities for protection or official complicity (GI-TOC 2025; UNODC 2025b).

Figure 2: A map of scam centres identified by UNODC in the Mekong region 2023–2025



Source: UNODC (2025b: 6)

These areas, many of which have been documented as previous sites of alleged illegal gambling operations (GI-TOC 2025), attract criminal scam operations for a range of reasons, such as their proximity to human trafficking routes and the ability to relocate compounds across borders following law enforcement crackdowns. Scam compounds may also be found in bigger towns and cities, housed in repurposed hotels, casinos, villas and apartment complexes, where they are enabled through structured protection arrangements with local officials and security forces (GI-TOC 2025).

More broadly, the pervasiveness of scam operations can be attributed to their replicable nature; they are not tied to complex logistics or fixed supply chains (Amerhauser and Goodwin 2026). They can spread across different jurisdictions, driven by criminal entrepreneurs who recognise favourable conditions and set up operations in new countries. Scammers also commonly exploit the instability created by geopolitical events (GI-TOC 2026). For example, fractured geopolitical landscapes create weak governance areas with poor regulatory oversight, within which scammers establish sites with opportunities for protection by corrupt officials (GI-TOC 2026).

Within these larger compounds, operations are typically organised through hierarchical structures: at the top, owners with local security or political connections; below them, operational managers; then, supervisors who coordinate the work of the teams. The latter are primarily responsible for the punishment and abuse of trafficked victims who are assigned as ‘team leaders’; these ‘team leaders’ then oversee 10 to 15 baseline ‘workers’ (OSCE 2026).

Compounds are reportedly self-contained in nature with designated areas for sleeping, eating and working, as well as widespread surveillance systems. Trafficking victims are seldom allowed to leave the premises, and digital control mechanisms such as facial recognition at compound entrances or surveillance cameras in work areas are used to prevent escape and maintain constant oversight (OSCE 2026).

Scam typologies

The types of scams undertaken in scam centres vary considerably. The table below provides a non-exhaustive overview of common scam typologies:

Table 1: Scam typologies often undertaken in scam centres

Type	Description
Romance scams	Often framed as an opportunity for a relationship and financial partnership, scammers build emotional trust with a victim before convincing them to transfer funds or invest in fraudulent schemes (USCC 2025; SEAPPI 2025).
Investment scams	Scammers lure victims with promises of high returns through fake or fraudulent schemes, often involving cryptocurrency (OSCE 2026; Smith 2023).
Deepfake extortion	Scammers use AI-generated images or videos of the victim to create blackmail material (Interpol 2025; OSCE 2026).
Task-based scams	Victims are recruited for microtasks, only to discover the tasks involve unlawful activity (Kreidler 2024; OSCE 2026).
Call centre fraud	Inbound/outbound fraud via voice over internet protocol or traditional phone systems (OSCE 2026).
Other typologies	Shopping scams; fake charity scams; business email compromise scams; advance fee scams and fake job scams (SEAPPI 2025).

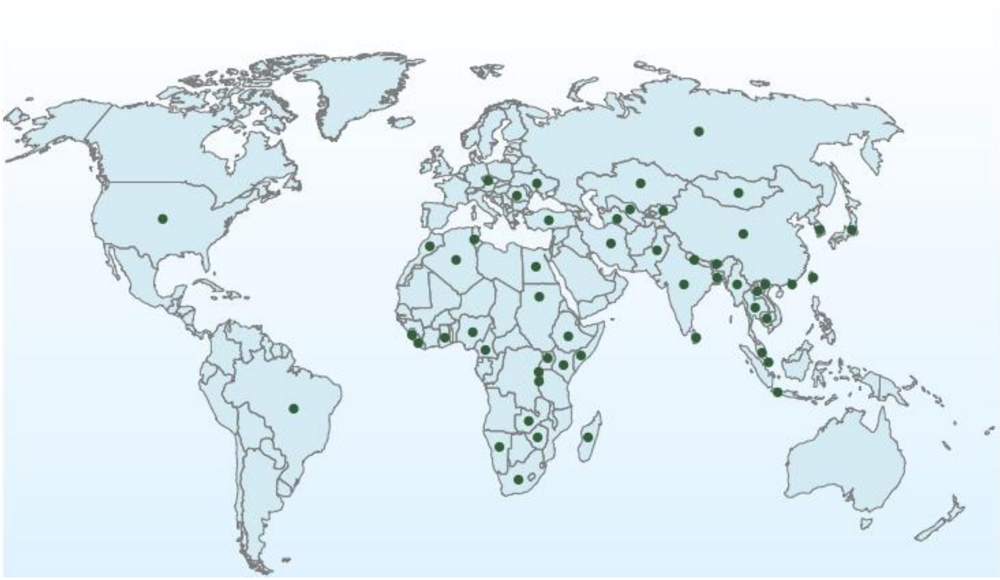
Technology has expanded the scam ecosystem, not only by enabling scammers to reach victims on a global scale but also by accelerating the technical sophistication of such scams (Amerhauser and Goodwin 2026). For example, artificial intelligence enables immediate translation, deepfakes and voice cloning and the ability to generate fraudulent documentation. These tools lower the technical barriers to highly personalised fraud, allowing scam operations to target victims across languages and jurisdictions with more speed and credibility (UNODC 2025c). Scammers also commonly steal funds via cryptocurrency, which enables rapid transactions and makes illicit proceeds difficult to trace. Fraud victims are often directed to transfer their funds from a normal bank account to a crypto exchange, where it is converted into cryptocurrency and then transferred on to fake investment platforms (OSCE 2026). While scam centres are generally associated with these sophisticated techniques, they also continue to conduct less sophisticated schemes, such as simple call centre fraud (OSCE 2026).

In addition, the accessible nature of information and communications technology makes the barriers of entry relatively low compared to other forms of criminal activity, such as commodity based (drugs, counterfeit goods) or human based (human trafficking, migrant smuggling) operations (Amerhauser and Goodwin 2026; GI-TOC 2026). A scam does not necessarily require significant enabling infrastructure but can be carried out with little more than an internet connection and a telephone.

Human rights abuses in scam centres

Scam compounds have become sites of serious human rights abuse, with victims often trafficked into these operations before being subjected to forced labour and coercive control once inside (Amnesty International 2025; Myat 2025; OHCHR 2023; 2026).

Figure 3: Origins of people identified in Southeast Asian scam compounds



Source: UNODC (2025b: 7)

Trafficked victims in scam compounds are primarily migrants in vulnerable situations who have been lured by the promise of well paying jobs, often through advertisements for professional roles such as programmers, marketers or HR specialists (Myat 2025; OHCHR 2023). These advertisements appear legitimate and deceive victims through elaborate procedures such as multiple-round interviews and language or competency tests (OHCHR 2023). Many escaped or rescued victims of scam operations have reported that they were recruited through fraudulent hiring processes (Amnesty International 2025; OHCHR 2023).

In addition to appearing legitimate, fraudulent advertisements often offer attractive and favourable conditions, such as high wages, regular bonuses and free accommodation and food (OHCHR 2023). Some migrants have also been offered a work visa on arrival, with some reporting that they were unaware they had even crossed an international border (OHCHR 2026). Survivors also report being sold into scam compounds, then sold on to others, indicating that victims are trafficked both into and between sites (Amnesty International 2025).

Once victims are trafficked into compounds, they are held against their will and forced to run the scams. They are sometimes made to sign contracts that obligate them to make a certain amount of profit for the compound, and to “agree” to punishments if expectations are not met (OHCHR 2026). In addition, costs such travel, training and living costs, and fines mean traffickers hold an ever-increasing debt over victims (OHCHR 2023).

Many are subjected to coercion, threats and physical or sexual violence, or they are trapped in debt bondage or stripped of their identity documents and forced to live in poor conditions (OHCHR 2023; 2026). Amnesty International's (2025) accounts of survivors' experiences in scam compounds in Cambodia indicate that victims reported experiencing several, and in some cases all, of the above abuses. In very extreme cases, deaths in compounds have been reported (OHCHR 2026).

Amnesty International (2025) outlines that violence carried out within compounds functions as a mechanism to prevent the spread of information out of compounds to maximise the extraction of labour and to establish a fearful environment that would prevent victims from contacting law enforcement or aid groups. There are documented acts of torture, including beatings, electrocution and solitary confinement, primarily if victims refuse orders or do not meet their scam target thresholds (OHCHR 2023). Victims also reported being forced to witness or conduct acts of torture themselves (OHCHR 2026).

Living conditions within sites are often cramped and unsanitary, with limited food and drinking water. These environments enable the spread of disease, with medical care inadequate or non-existent, further worsening conditions (OHCHR 2026). Victims also describe extreme sleep deprivation, being forced to work over 16 hours (and sometimes up to 19 hours) on a daily basis without any days off.

Reports also indicate that victims are subject to sexual violence, including rape as well as sex trafficking, commonly as a punishment for not meeting expected targets (Kelliher 2026; OHCHR 2023). Gendered exploitation is also commonly reported, including sexual attacks, forced abortion, abortion related deaths, lack of access to sanitary products and verbal abuse (Kelliher 2026). Kelliher (2026) notes that compound operators permit men to rape female victims as a reward for successfully completing lucrative scams.

Individuals that escape or are freed from compounds are often not treated as victims of human trafficking. They are subject to police arrest and immigration detention for periods of up to several months (OHCHR 2026). Victims are then commonly extorted by police or immigration officers and subjected to a range of fines and penalties. Should victims manage to return to their lives, they often do not have access to support services, resulting in severe mental health problems and/or financial struggles (OHCHR 2026).

Corruption and scam centres

Corruption is widely recognised as a "critical enabler of organised crime, allowing criminal networks to infiltrate institutions, evade law enforcement, and expand their influence across political, economic, and social domains" (EUROPOL 2025: 28–29). This issue of corruption is highly prevalent in scam operations, acting as a critical enabler of scam centres, as well as for human rights abuses, such as human trafficking (Amerhauser and Goodwin 2026; UNODC 2025a; OHCHR 2026). It is widely understood that large-scale operations could not function without some form of official complicity or protection (UNODC 2025a). Their ability to maintain operations is largely dependent on how well they embed themselves into local political and economic contexts. A well established and successful scam centre has likely forged structured arrangements with local criminal groups or elites, law enforcement officers or high-level officials, such as judges[1] or government officials (Amerhauser and Goodwin 2026). High-level protection of scam compounds normally involves structured arrangements with officials centred around security or protection, land or building leases, or financial agreements with law enforcement, military or other officials, an approach where a cut of the profits are given or bribes are paid to officials to enable operations in some capacity (Amerhauser and Goodwin 2026; UNODC 2025a).

Loughlin (2026: 11) argues that "elite brokerage and patronage and uneven economic growth" are often the institutional prerequisites characteristic of politically embedded scam operations. In these contexts, power is exercised through personalised networks and discretionary authority (Loughlin 2026). Political loyalty is maintained by granting access to rents, including land concessions, business licences and police protection (Hughes 2020). The form political embedding takes varies across institutional contexts (Loughlin 2026).

In Myanmar scam operations are embedded in systems characterised by contested sovereignty: shaped by civil war, militarised state-building and ceasefire arrangements (Loughlin 2026). In such environments, armed groups and militia-business networks police, tax and licence economic activity with social legitimacy and state support, creating the space and opportunity for armed group or militia led scam operations to become politically embedded (Loughlin 2026). In Cambodia, political embedding operates through a different set of arrangements and developed over time as a result of government relationships with business elites. Here, elites have at times funded political movements in return for access to state contracts, regulatory protection and monopoly concessions (Loughlin 2024a). Investment in casinos, online gambling and real estate was channelled through politically connected business networks. Scam

---

[1] The US Department of State (2023) reports that some judges or prosecutors have allegedly accepted bribes in return for the dismissal of charges, acquittals and reduced sentencing linked to scam operations in Cambodia. In addition, corrupt officials have reportedly halted progress in cases where the perpetrators allegedly had political, criminal or economic ties to government officials (US DoS 2023).

operations were later incorporated into such developments owned by state-linked elites and as a result were protected by local officials and secured by private security firms, embedding them within the same patronage structures that governed the earlier forms of economic activity (Loughlin 2026).

In Ukraine, it has been reported that some scam centres offered police between US$10,000 to US$15,000 per month for protection services. In exchange for such money, law enforcement officers may allow the scam centre to operate without legal scrutiny or give warning of potential raids or other monitoring activities, giving centres time to prepare or relocate (Amerhauser and Goodwin 2026; OHCHR 2023). In Southeast Asia, some compounds have even been located directly next to police stations (Amerhauser and Goodwin 2026; GI-TOC 2025).

Corruption to enable scam centres may also be low-level and more immediate, such as bribes paid to police officers in situations where operations have been raided or uncovered (Amerhauser and Goodwin 2026). These types of transactions have been documented in Nigeria and Southeast Asia where detained criminals pay officers to let them go or scam centre managers pay law enforcement officers who visit scam centres on an ad hoc basis to turn a blind eye (Amerhauser and Goodwin 2026).

Corruption-enabled scam operations

Scam operations and structured arrangements with the Karen Border Guard Force in Myanmar

There has been a major surge in cyber scam operations in Myanmar since the military's coup in 2021, which saw the expansion of organised crime groups around Myawaddy, the Thai border, and in parts of Shan state. The Myanmar military has been reported as a key enabler of organised crime in these areas and supports and protects the Karen Border Guard Force (BGF), a militia that is alleged to conduct cyber scam operations and enables criminal organisations to operate in eastern Myanmar, through which the Myanmar military receives a cut of profits (Justice for Myanmar 2025).[2]

Prominent scam compounds in these areas included Dongmei Park, KK Park and Huanya City (Watanabe 2024). These sites likely housed tens of thousands of trafficked workers, many of whom were trafficked out of China, Southeast and South Asia, the Middle East, Africa and Latin America. Justice for Myanmar (2025) notes that these operations would not be possible without structured arrangements with the Myanmar military, militias under its command and their associates.

---

[2] The US DoT (2025a) noted that the Karen BGF had changed its name to the Karen National Army in March 2024 "in an effort to distance itself" from the regime, but has had continued cooperation with the Myanmar military as recently as September 2024.

The Karen BGF reportedly plays a key role in conducting and enabling scam centre operations in these areas, distributing fuel and electricity for scam operations as well as facilitating human trafficking and smuggling across the Thai border (Justice for Myanmar 2025). Bayer et al. (2024) note that KK Park security was provided by the Karen BGF, and European Union sanctions were applied against Karen BGF Lieutenant Colonel Mote Thone (or Mote Thun) and Major Saw Tin Win, due to their involvement in the control of KK Park, including for the supply of electricity and fuel to scam operations (Justice for Myanmar 2025). In addition, the BGF Colonel Saw Min Min Oo reportedly sits on the board of directors for a company behind the establishment of the Shwe Kokko scam centre in Myawaddy. Following extensive reporting linking the Shwe Kokko SEZ to human trafficking, forced criminality and brutality, the UK sanctioned Saw Min Min Oo and two other affiliates in 2023 over their connections to the project (OFSI HMT 2023). Annual profits earned from the scam operations are substantial, with Shwe Kokko alone reportedly generating US$192 million a year. Reporting indicates that half of these profits go to the Karen BGF and half to the Myanmar military (Justice for Myanmar 2025). USIP (2024) reporting indicates that Shwe Kokko specifically acts as a hub for relationship based investment scams, and the US Department of the Treasury implemented sanctions against the Shwe Kokko area due to the prevalence of virtual currency investment scams targeting US citizens (US DoT 2025b)

It seems that high-profile criminals also reached structured agreements with the Karen BGF for the purposes of scam operations. For example, evidence shows that in 2019, Wan Kuok-koi, nicknamed Broken Tooth, established the Dongmei Zone near the Thailand-Myanmar border in agreement with the Karen BGF (USCC 2025). This area was initially purported to be a high-end tourism project, but instead saw the construction of a multitude of scam compounds (USCC 2025). The Council of the European Union (2024) outlines that Mote Thone controlled Broken Tooth's scam compounds as well as other compounds located in the Dongmei Zone.

The political embedding of scam operations in locations such as Myawaddy can be explained by the presence of non-state armed groups that act as de facto governing authorities and directly operate or facilitate scam centres within their territories (Loughlin 2026). These groups developed their own bureaucracies, policing and taxation systems, giving them state-like control over the local economy, mobility and cross-border trade. Cyber scam operations have proliferated in these areas under militia rule, becoming embedded in systems of territorial control and revenue extraction (Loughlin 2026). The Karen BGF reinforces state control in contested border areas while maintaining its own sphere of authority. Partnered with Chinese investors and criminal groups to leverage their position, they allegedly established scam hubs in, for example, the Shwe Kokko area, which were protected by armed guards, power and infrastructure. Profits from these operations, allowed the BGF to expand its force, cultivate patronage and independently finance its weapons, reducing reliance on established relationships with other groups (Loughlin 2026). The Karen BGF was therefore positioned both as a military auxiliary and an autonomous economic actor. Revenues from these operations altered the landscape for bargaining between the military, armed groups and local intermediaries, ultimately reshaping Myanmar's political settlement (Loughlin 2026).

Georgian officials' alleged scam centre operations

In 2022, a whistleblower who worked as an IT specialist for a major scam network in Georgia, revealed the details of a state-facilitated criminal syndicate. He outlined specific high-ranking officials and elites who allegedly enabled and protected different scam networks (TI Georgia 2026). His testimony indicates that Ucha Mamatsashvili, the cousin of informal ruler Bidzina Ivanishvili, received a 5 per cent cut from illegal scam call centre profits, alongside the head of the state security service (SSS), Grigol Liluashvili. The whistleblower's accounts also implicated former prosecutor general Otar Partskhaladze, claiming he was in charge of a large network operated by the Mikadze Brothers, prominent figures in Georgia's organised crime industry (TI Georgia 2026). Tbilisi Mayor Kakha Kaladze was also alleged to have protected certain large offices associated with scam centres. Investigations by OCCRP found that a Tbilisi based call centre, which generated US$35.3 million between 2022 and 2025, was located just metres from the SSS headquarters. In addition, Georgian Dream Party MP Isko Daseni allegedly offered political protection, and his son allegedly supplied software used to manage fraud victims. Former high-ranking interior ministry official Mindia Lordkipanidze, was also accused of using a private security firm as a means to physically protect scam centres and intimidate employees (TI Georgia 2026).

In late 2025, Georgian law enforcement authorities detained the SSS head, Grigol Liluashvii, after he was accused of taking substantial bribes in exchange for protecting illegal scam centres that targeted victims around the world (Civil.ge 2025; Messick 2026; OCCRP 2025).[3] Reporting indicates that protection for the network involved tip-offs or the shielding of call centres from law enforcement interference (Business Media 2026; IPN 2026). For example, former head of the Georgian financial police, Soso Ramishvili, claims Grigol Liluashvili gave him information about the addresses of alleged call centres, but once law enforcement arrived, the sites had been cleared out, indicating possible prior warning to the operators (Business Media 2026). Alleged protection was carried out through another one of Grigol Liluashvii's cousins, Sandro Liluashvili, who reportedly channelled approximately US$1.37million in bribes to Grigol (Civil.ge 2025). Civil.ge (2025) and Messick (2026) report that a large portion of the illicit revenue generated by call centres were used to finance Dream Party operations, various opposition media outlets, loyalty networks and the "broader survival machinery of the ruling system".

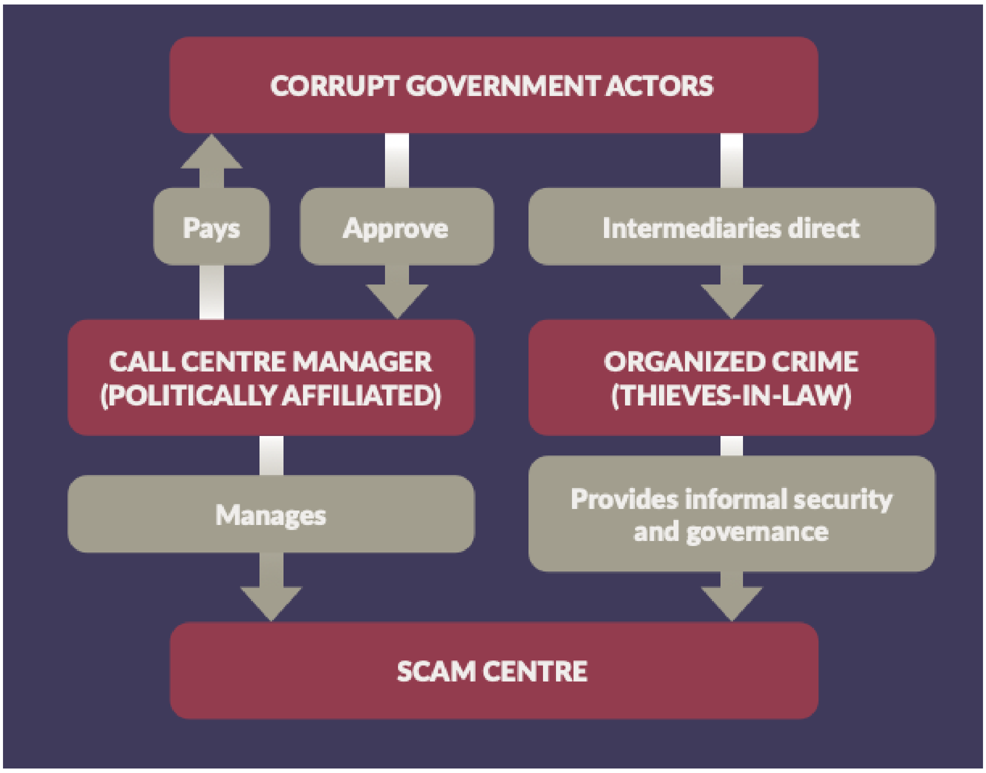
In a separate interview, Givi Targamadze, a former MP who chaired the defence and security committee in Georgia, claimed that call centres initially emerged in 2013/2014, connected to former prosecutor general Otar Partskhaladze and the Mikadze brothers, and later grew into a more structured and organised network (Messick 2026). Messick (2026) outlines that this network was organised in such a way that those with the right funding, connections and political cover could easily enter the business.

[3] At the time of writing, the case is still ongoing in court.

Call centre operators, acting on instructions from management, persuaded victims to invest through fake trading platforms, including via cryptocurrency (IPN 2026).

The scam centre ecosystem in Georgia gained worldwide notoriety following a body of investigative reporting, including the investigations documented above, which exposed large-scale networks operating with a high degree of sophistication (Amerhauser and Goodwin 2026). Due to the reporting, it is well understood that these networks were afforded high levels of institutional state protection under a quid pro quo in which corrupt officials provided protection while undertaking a leading role in the establishment and subsequent control of scam centres (Amerhauser and Goodwin 2026).

Figure 4: Model of the scam centre system in Georgia, based on October 2025 data



Source: Amerhauser and Goodwin (2026: 28).

Despite the arrests of high-profile officials involved in the operations, Georgia's scam centre ecosystem and many of the identified networks reportedly remain active (TI Georgia 2026). The testimony alleges that more low-level operators were arrested while the organisers remained largely untouched.

US-sanctioned Cambodian senators linked to hotels, resorts and casinos housing cyber scam operations

Scam compounds have become increasingly prevalent across Southeast Asia, with Cambodia emerging as a central hub in the regional scam economy (Dickson and

Quitzon 2026). Dickson and Quitzon (2026) report that senior government officials and business elites control, enable and benefit from scam compound operations.

In 2024, the US Department of the Treasury's Office of Foreign Assets Control sanctioned Cambodian senator and businessman Ly Yong Phat, his conglomerate LYP Group, and O-Smach Resort for their role in human rights abuses related to human trafficking and forced labour for the purposes of scam operations (US DoT 2024). Between 2022 and 2024, O-Smach Resort, which is reportedly owned by Ly Yong Phat via his LYP Group, was investigated by Cambodian authorities and publicly reported for systematic human rights abuses. Reports indicated that victims were lured to the resort with fraudulent employment opportunities, had their phones and documentation taken from them once they arrived and were forced to run scam operations (RFA Khmer 2025; US DoT 2024). Reports also point to physical violence such as beatings and electric shocks, cases where victims were forced to pay a large ransom and threats of being sold to other scam networks (US DoT 2024).

Figure 5: The O-Smach resort, reportedly owned by Cambodian tycoon Ly Yong Phat, in Oddar Meanchey province, Cambodia.

Source: RFA Khmer (2025)

Sims (2024) notes that Ly Yong Phat allegedly provides significant political cover to a range of scam operations, ensuring law enforcement do not interfere, and reportedly rents his network of properties to criminal organisations that undertake human trafficking for the purposes of scam operations. Kennedy and Southern (2023) report that victims have independently alleged to have witnessed high-ranking police officers entering the premises to collect bribes. One victim reported that an operation manager pays US$30,000 per month to local police for protection (Kennedy and Southern 2023).

However, despite documented evidence of legitimate investigations by authorities (see US DoT 2024) and an arrest warrant issued for Ly Yong Phat by Thai police (see Strangio 2025), the sanctions imposed against Ly Yong Phat were decried by the Cambodian government, with its foreign minister stating the treasury's action was "based on unconfirmed reports of forced labour linked to online investment scams" as well as "politically motivated" (Cheang and Peck 2024). At the time of writing, Ly Yong Phat still serves as a senator in Cambodia and recently voted "for a new law, which the Cambodian government says will harshly punish those involved in scamming" (Head et al. 2026). In terms of investigations into O-Smach resort, Cambodian authorities have reportedly raided the site and rescued trafficking victims on at least two occasions, though Ly Yong himself has faced no trafficking charges (Brook 2024). On site, authorities found fictitious identity scripts for romance scams, as well as American SIM cards (Wu 2026). US DoT (2024) similarly identifies investment fraud schemes as operating at the site.

The US Treasury Department also sanctioned senator Kok An for his role in scam centre networks that operated out of casinos and office parks, from which illicit revenues were laundered (Greig 2026; US DoT 2026). Kok An has political connections with former Cambodian prime minister Hun Sen and current prime minister Hun Manet, connections he has reportedly used to grow his empire of casinos, hotels and businesses (Greig 2026). Crown Resorts is cited as his flagship company, a firm that owns casinos, resorts and hotels in many cities along Cambodia's border. Grieg (2026) notes that these locations are used to house scam operations, from which Kok An reportedly derives rental income and provides other services, such as security. Grieg (2026) reports that many scam compounds in Cambodia are connected to casinos, from which the revenues generated from the operations can be easily laundered.

Sims (2025) argues that the prevalence of state-enabled cybercrime in Cambodia is linked to the existence of an embedded kleptocratic system. He notes that this kleptocratic system operates through several mechanisms that enable and sustain Cambodia's cybercrime and scam ecosystem:

- **Show crackdowns**: show crackdowns are where law enforcement performatively raids scam operations to relieve pressure from the international community and consolidate power among only the most well-connected elites. Sims (2025) notes that, in 2022, Cambodian law enforcement raided a number of scam compounds, representing the first industry-wide crackdown on scam operations. However, it later became apparent that many compounds were warned ahead of the crackdowns.

- **Local direct investors**: in Cambodia, an elite class of oligarchs hold ownership stakes in the infrastructure and technology used for cybercrime activity. Figures in this class include, according to the reporting above, the aforementioned Ly

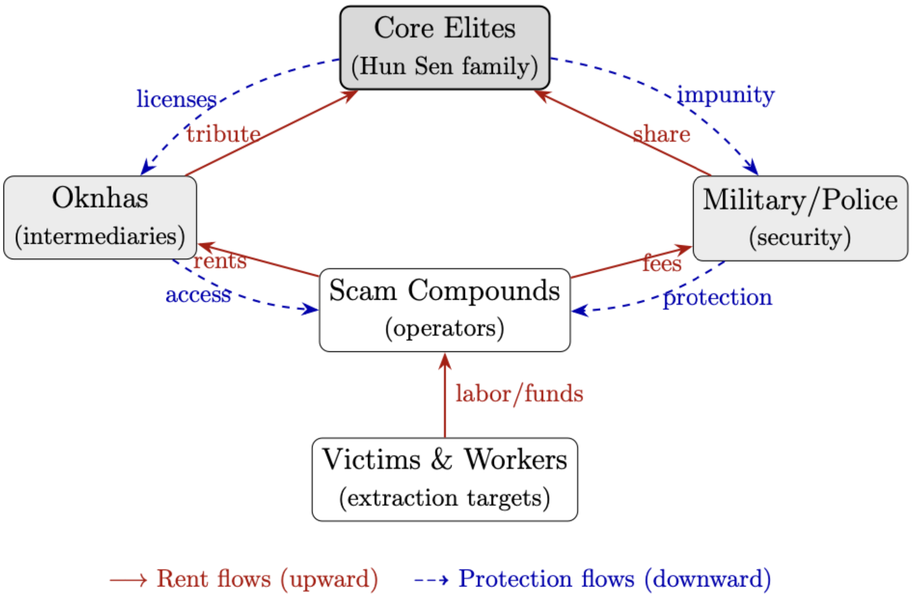
Yong Phat among other high-profile political or politically connected elites. Sims (2025) notes that, in general, each scam compound appears to be connected to at least one local oligarch-patron who, for example, leases the land or property or offers politically influenced shelter from law enforcement.

- **Foreign investors**: many cybercriminals and key investors in Cambodia's scam economy are not from Cambodia but from China (Sims 2025; USCC 2025). USCC (2025) notes that Chinese criminal organisations operate extensive scam operations across Southeast Asia. The US-China Economic and Security Review Commission, an independent commission of the United States government legislative branch, claims that when these criminal syndicates were establishing enterprises in Southeast Asia, they developed relationships with officials eager to promote China's Belt and Road Initiative. Syndicates then invested large sums into scam infrastructure projects backed by the initiative and associated officials, embedding Chinese state-backed criminal operations into Southeast Asian countries such as Cambodia (USCC 2025). It is important to note, however, that according to evidence reviewed by the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (2026), such scam operations in Cambodia are not state-directed. Rather "CCP-linked criminal capital became intertwined with elite protection networks and development projects" (Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party 2026: 14).

- **Key propagandists**: elite actors also support the scam ecosystem by leveraging the state to downplay and obfuscate the realities of major criminal industries (Sims 2025). Sims (2025) notes that much of the Cambodian government's official responses to scamming and other criminal industries takes the form of overt propaganda.

- **Public official enablers**: another key group of state-linked cybercrime actors in Cambodia are public official enablers. The case of Dy Vichea could provide an illustrative example. Vichea is the brother-in-law of Cambodia's Prime Minister Hun Manet, and the son of late national police chief Hok Lundy. Vichea controlled a commercial gambling unit within Cambodia's national police force. Complaints of human rights abuses within scam compounds were directed to the unit, but reports allege it functioned as a protective unit, sheltering scam operation owners from investigations or allegations (Sims 2025). Official enablers also reportedly extract rents from owners in exchange for tip-offs before raids. For example, Vichea allegedly demanded US$100,000 to raid a compound in Sihanoukville, with assurance that the owner would be given warning before the raid took place. This, if true, indicates a performative enforcement action which relieved pressure to act, while allowing the scam operation to continue elsewhere.

Figure 6: Patronage network and rent flow structure in Cambodian scam operations according to Luoluo



Source: Luoluo (2025: 11)

This rent-seeking mechanism comprises several functions:

- Entry rents correspond to upfront costs, such as for obtaining permission to operate via land lease fees, security operation fees and fees for access to telecommunications (Luoluo 2025).
- Operational rents correspond to daily operational costs, such as protection payments, law enforcement arrangement fees and costs for handling escaped workers or those who contact authorities. For the latter, OHCHR (2023) outlines reports of rescue fees when victims' families or international aid organisations contact authorities for assistance.
- Exit rents are necessary for responses to increased political risks, such as compound relocation, operational "clean-ups", transferring victims or payments to officials for the aforementioned purposes (Luoluo 2025).

Luoluo (2025) notes that this rent-seeking system is only accessible to criminal activities that are able to afford layered rent payments. Small-scale operations, therefore, are less able to access this market, giving large criminal organisations the ability to monopolise the scam industry.

Human rights abuses facilitated by corrupt officials

It is crucial to highlight that criminal networks that undertake scam operations also engage in human trafficking for forced criminality enabled by corruption, with corrupt law enforcement officers, border security and other government officials enabling this exploitation (OHCHR 2026; Tower 2026; UNODC 2025a). Corruption is a documented enabler of human trafficking at every stage of the scam operation process as well as for all forms of trafficking. UNODC (2025a: 34) states that, alongside border controls and police stations, “labour inspectorates, recruitment agencies, hotels, factories, the agricultural industry and construction companies” are all vulnerable to bribery that facilitates “recruitment, transportation, control and exploitation of trafficking victims”.

Victims report corrupt practices such as collusion in trafficking by immigration officials (OHCHR 2026). Some reported being identified or fast-tracked by officials who moved them faster through immigration lines and seemed to alert traffickers to their presence. Others said they were met before immigration control by border officials, directed to specific lines and accompanied through border control. In one case, a victim was allowed to leave his country of origin despite an emigration restriction on his passport; on arrival in the destination country, a border official directed him to a compound recruiter.

There have also been reports of escaped victims being subjected to exploitation by corrupt officials (Amnesty International 2025; OHCHR 2026; Tower 2026). For example, Cambodian government officials reportedly took bribes from “rescued” victims in exchange for allowing them to avoid immigration detention and leave the country (Amnesty International 2025). One victim said that police officers who removed him from a scam centre demanded US$100 for transportation and a further US$100 to make a phone call (OHCHR 2026). Another reported that, during the rescue process, a police translator instructed him to write a statement denying that he had been abused or beaten while held in the compound (OHCHR 2026).

Corruption and money laundering in scam operations

Money laundering is a central function and core enabler of corruption, organised crime and cybercrime, acting as the financial lifeline that gives criminal enterprises the means to sustain their activities (UNODC 2025a). Technological and structural developments in global finance, such as via the popular emergence of crypto currencies, offshore banking jurisdiction and informal value transfer systems, have given scam operations new and emerging ways to launder proceeds (Loughlin 2026). While not exhaustive, money laundering networks comprise legal entities including professional “gateway” companies, high-risk virtual asset service providers (including currency exchanges, decentralised exchanges and crypto mixers) and money mules who are either deceived into providing access to their bank accounts or knowingly sell them to criminal groups (GI-TOC 2025).

While the evidence to suggest corrupt actors directly facilitate the laundering of scam proceeds is unclear, there is reported evidence that the scam operations facilitated by corrupt actors launder their proceeds through emerging and sophisticated methods (APG 2025). This laundering infrastructure serves two purposes: concealing the origins of illicit funds and channelling scam proceeds back into host country political economies through investment, campaign finance and discretionary patronage (Loughlin 2026). According to Loughlin (2024), scam proceeds in Cambodia have supported elite property developments, political campaigns and helped purchase titles within the ruling party. These dynamics constitute a transnational system where scam compounds generate illicit proceeds, laundered through offshore networks and protected by political arrangements in which access is exchanged for rents (Loughlin 2026).

UNODC (2025a) note that the proceeds of cybercrime can be laundered in many different ways. One technique is to steal or fabricate identity documents for the purposes of opening bank accounts or crypto wallets, which then receive and transfer illicit funds. The pseudo-anonymity of crypto assets make tracing the origin and destination of funds difficult for authorities. Mechanisms such as un-hosted wallet addresses, mixers, tumblers and privacy coins are used to further obfuscate the proceeds of cybercrime operations (UNODC 2025a).

Another method is the use of money mules, shell companies, legitimate businesses and financial institutions to store, layer and conceal illicit funds.[4] In Cambodia, for example, casinos are frequently cited as key sites housing laundering operations (Amnesty International 2026; US DoT 2026). US DoT (2026) states that nearly all major scam centres in Cambodia are connected to casinos, which serve to launder scam proceeds. Sims (2025) notes that the gambling industry's secondary banking system functions as a "mixer", co-mingling funds from multiple sources. Whitehouse (2025) reports that Cambodia "pays virtually no attention" to casino junket operators, despite the widespread misuse of these sites for laundering purposes. Money laundering may also occur at the same sites where scam operations are conducted (Amnesty International 2026). For example, at the Crown Resorts complex, rescued victims' reports indicate that workers were forced to open bank accounts for the likely purposes of laundering scam proceeds, acting as money mules for the criminal enterprises who imprison them (Amnesty International 2026).

The widespread use of money mules and legal entities to launder scam proceeds is partly enabled by weaknesses in financial sector regulation (APG 2025). Weaknesses in

[4] Professional intermediaries, including lawyers, accountants, trust and company service providers may knowingly or inadvertently support the creation and administration of these structures (APG 2025).

customer due diligence and know-your-customer procedures allow criminal actors to establish and use various mule accounts even when existing accounts associated with similar criminal activity has been identified by authorities (APG 2025). Criminal organisations also exploit unlicensed or unregulated remittance services to launder scam proceeds due to weak regulations and poor cross-jurisdictional oversight (APG 2025).

Enabling factors

The role of corruption in scam operations can be attributed to a series of enabling factors, including weak governance, regulatory gaps, geopolitical and conflict related factors, and the existence of embedded relationships between organised crime groups and state officials (Amerhauser and Goodwin 2026; GI-TOC 2025; Loughlin 2026; OHCHR 2023; OSCE 2026; UNODC 2025a; b). Areas of weak governance create permissive environments within which criminal enterprises are able to entrench and expand their operations (USIP 2024). In these environments, regulatory systems become fragmented, enforcement is applied selectively and state authorities are co-opted by criminal activities for private gain (UNODC 2025a). Over time, this creates favourable conditions for a small group of elites, while others disadvantaged. They establish a culture of impunity where corruption is normalised, further entrenching the systems that enable criminality and exploitation. Governance operates through personal networks and discretionary power (Loughlin 2026). Political loyalty is maintained through access to rents, including land concessions, business licences and police protection, with the same arrangements governing illicit markets (Hughes 2020). Criminal networks often disperse to and target underprepared or vulnerable regions, such as areas in parts of Africa, the Middle East, select Pacific Island nations, South America, South Asia and Eastern Europe (Amerhauser and Goodwin 2026; UNODC 2025a).

Corruption in scam operations is also enabled by long-standing and embedded relationships between organised crime groups and state officials, which are sustained by recurring patronage and rent-sharing arrangements (Loughlin 2026). In these arrangements, criminal groups generate illicit income from scam operations, while officials use their public authority to protect their activities (Loughlin 2026). Loughlin (2026) argues that countries characterised by elite brokerage, patronage and uneven economic growth are often more likely to see these relationships emerge. In other words, patronage based political systems create opportunities for organised crime groups to build mutually beneficial relationships with state officials. Many of these relationships have been cultivated over a long period of time, meaning corrupt protection is often entrenched in the operation of scam centres in these contexts (Loughlin 2026).

Legislative gaps also enable corruption in scam operations. In such contexts, corrupt officials and associated actors exploit these gaps to facilitate the movement, confinement and exploitation of victims while shielding compound operators from scrutiny (UNODC 2025b). Six of ten ASEAN member states are yet to criminalise bribery in the private sector or have laws which are insufficient in scope, meaning scam centres that are fronted as legitimate businesses, such as casinos, hotels or office parks, may not be subject to effective anti-bribery enforcement (UNODC 2025b). Only three out ten ASEAN member states have established dedicated whistleblower protection legislation. Most ASEAN member states have not yet put in place sufficient measures to ensure transparency over legal persons and arrangements, including clear mechanisms for verifying, sharing and keeping beneficial ownership information up to date (UNODC 2025b). These gaps give criminal actors the ability to sustain scam and money laundering operations through the use of complex corporate structures and shell companies. Notably, eight of ten ASEAN member states do not have adequate legislation for the liability of legal persons, with some regions unable to fully recognise legal persons as criminal actors. Out of these eight, seven lack effective, proportionate and dissuasive sanctions for legal persons (UNODC 2025a).

In addition, while the majority of ASEAN member states have national legislation aligned with the UN Trafficking in Persons Protocol, reports indicate that some domestic laws still fall short of international standards, or that existing legal provisions are not being applied to cases involving trafficking into online scam operations (OHCHR 2026). At the national level, concerns include failures to identify, assist and provide remedies to trafficked persons; protect victims from prosecution; and prevent corruption and official complicity in trafficking cases (OHCHR 2026).

Due to the legal and regulatory gaps in SEZs, they may harbour corruption-enabled scam operations. These areas are primarily designed to stimulate trade and investment and to create jobs through trade benefits, deregulation and other investment or tax concessions (UNODC 2025a). However, limited regulation and oversight of SEZs create the conditions for illicit trade, criminal enterprise and create an enabling environment for corrupt arrangements (UNODC 2025a). As a result, sites of corruption-enabled cybercrime operations may be hosted in SEZs, especially in Southeast Asia (UNODC 2025a). For example, the MDS Thmorda SEZ in Cambodia, the Golden Triangle SEZ in Laos and Clark Freeport SEZ in the Philippines, among others, have all been cited as locations that house scam operations (GI-TOC 2025). More broadly, the existence of casinos and online gambling companies in SEZs is understood to increase the risk of criminality. In 2021, “there were approximately 340 licensed and unlicensed casinos across Southeast Asian SEZs, some of which were used for money laundering, illegal gambling and, more recently, cyber scams involving forced criminality”. The reported involvement of Chinese-owned development, management and security companies in these areas may also explain this increase (GI-TOC 2025: 8).

Corruption-enabled scam operations are also often located in high-risk border areas, conflict affected areas or areas with contested authority (OHCHR 2023). For example, the military coup and armed conflicts in Myanmar have given actors, reportedly including the Karen BGF, opportunities to enable and control scam operations (Justice for Myanmar 2025; OHCHR 2023). Many scam centre operations in Myanmar exist in border areas that are weakly regulated and have poor or minimal law enforcement structures, oversight and accountability (OHCHR 2023). Connected to this is the problem of international or cross-border law enforcement cooperation. When political tensions rise between jurisdictions, cooperation is inevitably hindered, making it harder to investigate and share intelligence on scam operations (Amerhauser and Goodwin 2026).

Mitigation measures

The scam centre industry is very diverse and adaptive in its nature and operations. It responds to both shifts in the global political sphere and innovates in its use of emerging technology and operational security. In addition, scam centres do not operate according to a single model; rather, they come in many forms and have different functions.

Despite this, scam centres generally do share a set of common components, meaning that, whatever form they take, policy responses can be structured around shared features. Amerhauser and Goodwin (2026) argue that the components that constitute a scam centre are what policy recommendations should focus on, rather than on single elements of a scam operation. With this in mind, below is a non-exhaustive list of mitigation measures designed to address scam centre operations generally and associated human rights abuses:

- **Strengthen international law enforcement and regional cooperation**: criminal scam networks operate across borders and can rapidly relocate scam operations between jurisdictions. In addition, many investigations are likely targeting the same criminal activities and individuals; therefore, stronger regional cooperation is essential to any effective response (GI-TOC 2025). It can enable authorities to more effectively share intelligence, resources and operational leads, thereby strengthening law enforcement efforts to address scam operations globally (Amerhauser and Goodwin 2026; GI-TOC 2026; UNODC 2025b).
- **Create safeguards for emerging technology**: as scam operations become more sophisticated and increasingly rely on new forms of technology, responses will need to draw on the combined expertise of governments, law enforcement agencies, technology companies and civil society. This should include stronger safeguards, public awareness campaigns and protective AI tools that can help detect and disrupt an ever-diversifying scam ecosystem (GI-TOC 2026; UNODC 2025a).
- **Identify entry points to create political will to address the problem of scam centres:** meaningful reform will depend on sustained political will, but governments should also identify entry points where action is already feasible. In the shorter term, this may include measures framed around reducing the economic costs of reputational damage to the country, which could attract broader support while creating space for more ambitious reforms over time (GI-TOC 2025; UNODC 2025b).
- **Develop and offer reintegration pathways and risk monitoring procedures for former trafficked scammers:** given their skills and experience, as well as difficult post-escape livelihoods, providing alternative work opportunities or other reintegration pathways is essential to reduce the risk that trafficked

survivors re-enter the scam ecosystem, whether through existing criminal networks or by establishing operations of their own (OHCHR 2023; 2026).

Corruption acts as a critical enabler of scam operations globally, especially for larger operations, which often require some form of political complicity or facilitation to be sustained (GI-TOC 2026; UNODC 2025a). Therefore, it is also important for responses to consider and develop policy recommendations for corruption-enabled scam operations. Several organisations outline recommendations designed to address the role of corruption in scam centres, as well as for corruption-enabled human rights abuses that intersect with such operations:

- **Use diplomatic and economic tools to disrupt politically protected scam centres**: where scam centres are sustained by political protection, target countries may be able to supplement criminal investigations with diplomatic or economic pressure, such as sanctions or extradition (Tower and Amerhauser 2026), on the jurisdictions that allow these operations to persist (GI-TOC 2026).
- **Prioritise strengthening governance in areas of weak accountability, such as border areas and SEZs:** governments must assert effective oversight in border areas and SEZs, especially where corruption in authorities is entrenched. This can include the displacement of criminal activities and should be paired with local economic development strategies to avoid further harm to communities. Such measures should also be supported by efforts to root out the corruption that has allowed scam operations to function without interference (GI-TOC 2025).
- **Criminalise corrupt acts and enhance other measures to address and prevent corruption**: many countries, especially in Southeast Asia, do not have adequate legislation to prevent corruption, such as for acts of bribery or to protect whistleblowers. This gives criminal actors incentives to engage in and sustain scam operations. It is therefore important that countries address these gaps by enacting effective anti-corruption legislation, which will prevent further legal and regulatory exploitation by scam operations (UNODC 2025b).
- **Identify and eradicate public sector involvement in human trafficking**: addressing corruption-enabled human trafficking is crucial not only for preventing further proliferation of the scam industry but also for ending the severe harms endured by victims lured into operations (OHCHR 2023; 2026). All public officials suspected of being implicated in trafficking and/or corruption that facilitates trafficking should be subject to investigation and prosecution in line with due process and fair trial standards (Amnesty International 2025; OHCHR 2023).
- **Support and protect the role of investigative journalism and civil society for the purposes of uncovering corruption in scam operations**: the Georgia case illustrates the crucial role of investigative journalism and civil society in uncovering politically embedded scam operations (TI Georgia 2026). Various mechanisms such as secure reporting channels and global advocacy networks are crucial for exposing corruption in these operations (Phongsathorn and Vlassis 2025). Amerhauser and Goodwin (2026) note that this role is becoming

increasingly challenging due to the passing of various forms of "foreign agents" laws in countries such as Georgia, which require civil society to disclose sources of foreign funding. In order to prevent silencing, punishing or excluding the voices that challenge, it is crucial that the international community supports and protects investigative journalism and civil society organisations in the pursuit of uncovering corruption, and speak out when these voices are persecuted for exposing corruption and organised crime, while providing safety to those forced to flee persecution (Phongsathorn and Vlassis 2025).

References

Amerhauser, K. and Goodwin, A. 2026. A World of Deceit: Mapping the Landscape of the Global Scam Centre Phenomenon.

Amnesty International. 2025. 'I Was Someone Else's Property': Slavery, Human Trafficking and Torture in Cambodia's Scamming Compounds.

Amnesty International. 2026. Cambodia: Casinos Get State Approval Despite Links to Human Rights Abuse At Scamming Compounds. Amnesty International, [online] 2 April.

Antoniuk, D. 2025. Georgia Arrests Ex-Spy Chief over Alleged Protection of Scam Call Centers. The Record [online], 26 December.

Asia Pacific Group (APG). 2025. APG Yearly Typologies Report 2025. November.

Bayer, J., Pineda, J. and Li, Y. 2024. How Chinese Mafia Are Running a Scam Factory in Myanmar. Deutsche Welle [online] 30 January.

Brook, J. 2024. EU, UN Reschedule Launch of Anti-Human Trafficking Project in Cambodia after Questions About Venue. AP News, [online] 1 May.

Business Media. 2026. According to Ramishvili's Testimony, the Financial Police Did Not Find Anything on the Spot At the "Call Center" Addresses Provided by Liluashvili – Prosecutor. BM, [online] 2 July.

Cheang, S. and Peck, G. 2024. Cambodia Decries US Sanctions against One of Its Top Tycoons Implicated in Forced Labor. AP News, [online] 13 September.

Civil.ge. 2025. Ex-State Security Chief Grigol Liluashvili Arrested on Bribery Charges. Civil.ge [online], 23 December.

Council of the European Union. 2024. Council Implementing Regulation Implementing Regulation (EU) No 401/2013 Concerning Restrictive Measures in View of the Situation in Myanmar/Burma. Brussels, 22 October.

Dickson, J. and Quitzon, J. 2026. From Fraud to the Frontlines: Scam Centers Caught in the Cambodia–Thailand Conflict. Center for Strategic and International Studies (CSIS), 15 January.

Ear, S. 2012. Aid Dependence in Cambodia: How Foreign Assistance Undermines Democracy. Columbia University Press.

Europol. 2025. The Changing DNA of Serious and Organised Crime: EU Serious and Organised Crime Threat Assessment.

Global Initiative Against Transnational Organized Crime (GI-TOC). 2026. Scam Centres: Combating a Global Phenomenon.

Global Initiative Against Transnational Organized Crime (GI-TOC). 2025. Compound Crime: Cyber Scam Operations in Southeast Asia.

Greig, J. 2026. US Sanctions Cambodian Senator for Millions Earned through Scam Compounds. The Record [online], 23 April.

Head, J., Luo, L., and Doksone, T. 2026. Fake Australian, Chinese and Brazilian Police Stations: BBC Goes Inside a Seized Scam Compound. BBC, [online] 7 April.

Hughes, C. 2020. 'Transitions from State "Socialism" in Southeast Asia', in T. Carroll, S. Hameiri and L. Jones (eds) The Political Economy of Southeast Asia: Politics and Uneven Development under Hyperglobalisation, pp. 111–30. Cham: Springer

International Crisis Group (ICG). 2024. Scam Centres and Ceasefires: China-Myanmar Ties Since the Coup.

International Labour Organization. 2025. ILO Indicators of Forced Labour 2025 Revised Edition.

INTERPOL. 2025. INTERPOL Releases New Information on Globalization of Scam Centres. INTERPOL, [online] 30 June.

Inter Press News (IPN) 2026. Prosecutor's Office: According to Witness Testimonies, the Majority of the “Call Centers” Belonged to a Group of Persons Who Financed Various Opposition Media Outlets, While the Relatively Smaller Portion of the “Call Centers” Was Patronized by Grigol Lil. IPN, [online] 18 February.

Justice for Myanmar. 2025. Who Powered the Expansion of Cyber Scams in Myawaddy? Justice for Myanmar, [online] 4 March.

Keeton-Olsen, D. 2022. After Malaysian Rescues from Cambodia, Politician Warns More People Trapped. VOD [Online], 20 April.

Kennedy, L. and Southern, N.P. 2023. ‘Just as Scared’: Cyberscam Victims in Cambodia Find No Freedom in Rescue. Al Jazeera [online], 24 November.

Kelliher, F. 2026. Trafficked, Beaten and Raped: Raids Reveal Scale of Abuse of Women in Asia’s Cyberscam Centres. *The Guardian,* [online] 29 June.

Kreidler, J. 2024. Task Scams Create the Illusion of Making Money. Federal Trade Commission, [online] 12 December.

Loughlin, N. 2024a. The Politics of Coercion: State and Regime Making in Cambodia. Ithaca, NY: Cornell University Press.

Loughlin, N. 2026. Digital Crime, Dirty Money and the State: Southeast Asia's Illicit Political Economy and the Rise of Cybercrime.

Luoluo, G. 2025. Predatory Enclaves: The Political Economy of Cyber-Scam Compounds and Mechanisms of State Capture in Cambodia.

Messick, R. 2026. Call Centers, Cash, and Power: Georgia’s Hidden Political Economy — Revised. Global Anticorruption Blog [online], 16 June.

Myat, S. 2025. Beatings, Torture and Electric Shocks: Freed Scam Compound Workers Allege Horrific Abuse. The Guardian [online], 25 February.

O’Bryan, J. 2025. What are Scam Centres – Explained in 30 Seconds. Guardian [online], 2 December.

Office of Financial Sanctions Implementation HM Treasury (OFSI HMT) 2023. Financial Sanctions Notice. 8 December.

Office of the OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings (OSCE). 2026. Trafficking into Cyber Scam Operations: Implications for the OSCE Region Exploratory Assessment. Vienna.

Office of the United Nations High Commissioner for Human Rights (OHCHR). 2026. “A Wicked Problem” Seeking Human Rights-Based Solutions to Trafficking into Cyber Scam Operations in South-East Asia.

Office of the United Nations High Commissioner for Human Rights (OHCHR). 2023. Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response.

Organized Crime and Corruption Reporting Project (OCCRP). 2025. Georgia Detains Ex-Security Chief over Alleged Bribes Tied to Global Scam Call Centers. OCCRP [online], 23 December.

Phongsathorn, P. and Vlassis, I. 2025. Shutting out the Light: the Voice of Civil Society is Being

Stifled in the Mekong Region. GI-TOC [online], 9 September.

Radio Free Asia (RFA) Khmer. 2025. Storming Past Guards, 60 Foreigner Workers Escape from Cambodian Casino. RFA [online], 6 January.

Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. 2026. Crime, Corruption, and Power CCP-Linked Transnational Crime and the Rise of a Distributed Threat to U.S. National Security. 19 May.

Smith, N. 2023. Crypto Prison Scams Pose a 'Serious and Imminent Public Threat', Interpol Warns. Telegraph, [online] 8 June.

Southeast Asia Public Policy Institute (SEAPPI). 2025. Towards an ASEAN Response to Scams.

Sims, J. 2025. Policies and Patterns: State-abetted Transnational Crime in Cambodia As a Global Security Threat. Humanity Research Consultancy.

Sims, J. 2024. The Sanctioning of Ly Yong Phat: Milestone or Mirage? The Diplomat [online], September 13.

Strangio, S. 2025. Thai Police Issue Arrest Warrant for Cambodian Tycoon Ly Yong Phat. The Diplomat, [online] 10 November.

The Economist. 2025. Online Scams May Already Be As Big a Scourge As Illegal Drugs. The Economist, [online] 6 February.

Tabahriti, S. 2026. UK Sanctions Cambodia-Based Scam Centre and Crypto Platform. Reuters, [online] 26 March.

TI Georgia (Transparency International Georgia). 2026. Georgian Dream and Scam Call Centers in Georgia.

Tower, J. G. 2026. Crime, Corruption, and Power: the Rise of CCP-Linked Scam Networks Targeting Americans and Threatening U.S. security. Testimony before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. GI-TOC.

Tower, J. and Amerhauser, K. 2026. 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, [online] 29 January.

United Nations Office on Drugs and Crime (UNODC). 2025a. The Nexus between Cybercrime and Corruption.

United Nations Office on Drugs and Crime (UNODC). 2025b. Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia.

United Nations Office on Drugs and Crime (UNODC). 2025c. Emerging Threats: the Intersection of Criminal and Technological Innovation in the Use of Automation and Artificial Intelligence in the Cybercrime Landscape of Southeast Asia.

United Nations Office on Drugs and Crime (UNODC) (undated) #TrappedInScamCrime Regional Campaign.

US-China Economic and Security Review Commission (USCC). 2026. Protecting Americans from China-Linked Scam Centers: An Update on Emerging Trends. Commission Spotlight, 5 March.

US-China Economic and Security Review Commission (USCC). 2025. China's Exploitation of Scam Centers in Southeast Asia. Commission Spotlight, 18 July.

US Department of the Treasury (US DoT). 2024. Treasury Sanctions Cambodian Tycoon and

Businesses Linked to Human Trafficking and Forced Labor in Furtherance of Cyber and Virtual Currency Scams. 12 September.

US Department of the Treasury (US DoT). 2025a. Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scam Operations. 5 May.

US Department of the Treasury (US DoT). 2025b. Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams. 8 September.

US Department of the Treasury (US DoT). 2026. Treasury Sanctions Cambodian Senator Kok An and Scam Center Network Defrauding Americans. 23 April.

US Department of State (US DoS). 2023. 2023 Trafficking in Persons Report: Cambodia.

United States Institute of Peace (USIP). 2024. Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security.

Watanabe, K. 2024. Militia as a Coercive Broker: Border Guard Forces and Crime Cities in Myanmar’s Karen Borderland. Global China Pulse [online], 21 November.

Whitehouse, D. 2025. FATF is Behind the Curve on Cambodia’s Cyber-scam Compounds. The Diplomat, [online] 18 July.

Wu, H. 2026. Inside a Huge Compound on Thailand-Cambodia Border Where 10,000 Workers Scammed People Globally. AP News, [online] 8 April.

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

Transparency International
International Secretariat
Alt-Moabit 96
10559 Berlin
Germany

Phone: +49 - 30 - 34 38 200
Fax: +49 - 30 - 34 70 39 12

tihelpdesk@transparency.org
www.transparency.org

transparency.org/en/blog
facebook.com/transparencyinternational
twitter.com/anticorruption