The Grey Zones of Southeast Asia

How scam compounds, trafficking networks and weak enforcement created a new exploitation economy

THE HUMAN TRAFFICKING BRIEFING

By Not For Sale

For leaders who know some issues are too important to ignore

Executive summary

Across parts of Southeast Asia, online fraud has developed into something more structurally important than a cluster of criminal scams. It now operates as a regional exploitation system in which deceptive recruitment, cross-border movement, confinement, forced criminality, money laundering, and regulatory fragmentation reinforce one another. The phrase “grey zones” is used here as editorial shorthand for the permissive environments that make this possible: places that are not simply outside the law, but where commercial development, weak oversight, political protection, illicit finance, and cross-border ambiguity overlap. That overlap, rather than physical remoteness alone, is what has allowed scam compounds to scale.

The scale is no longer plausibly described as marginal. In April 2025, UNODC said scam centres across Southeast Asia were generating just under US$40 billion a year, and that a potentially irreversible spillover was under way as criminal groups shifted, adapted, and expanded beyond the Mekong into other regions. In February 2026, the UN Human Rights Office said hundreds of thousands of people from dozens of countries had been trafficked into entrenched scam operations, mostly in Southeast Asia but increasingly beyond it.

The key analytical mistake is to treat this as either a trafficking story or a cybercrime story. It is both at once. INTERPOL’s June 2025 update is especially useful on this point: one victim group is trafficked into compounds and coerced into fraud, while another victim group is defrauded online through romance scams, investment fraud, impersonation, and related schemes. That dual-victim structure helps explain why the issue slips between policy silos and why responses often address one side of the model while leaving the rest intact.

The most important conclusion of this briefing is simple. The real problem is not only the compounds. It is the broader system that makes compounds viable: permissive special zones and border economies,

deceptive labour channels, adaptable criminal service markets, and financial rails capable of laundering proceeds at scale. As long as intervention focuses mainly on raids, rescues, or single-site closures, the model will survive by moving, rebranding, and reconfiguring. That is why serious readers need to understand the architecture, not just the headlines.

Why this briefing now

This issue has reached a point where it can no longer be treated as a regional curiosity. UNODC has described scam centres and related illicit online marketplaces in Southeast Asia as having global implications, while INTERPOL says the trafficking pipeline has already internationalised, with victims from 66 countries identified by March 2025 and no continent untouched. OHCHR likewise says the industry has spread beyond the Mekong to parts of South Asia, the Pacific, the Gulf, West Africa, and the Americas.

Recent enforcement developments show that governments now recognise the seriousness of the threat, but they also reveal its resilience. Reuters reported in March 2026 that the UK sanctioned a Cambodia-based scam compound operator and a Chinese-language crypto marketplace accused of facilitating online fraud. AP reported on 30 March 2026 that Cambodia's parliament passed a new anti-scam law with penalties reaching life imprisonment in the most serious cases. Those moves matter, but they also underscore that the model had already grown large enough, visible enough, and diplomatically costly enough to force a legislative and sanctions response.

What the reader needs to understand first

The first distinction is conceptual. These sites are often described as scam centres, scam compounds, or scam farms, but those labels can obscure what they are operationally. They are not simply buildings in which fraud happens. They are labour sites, coercive workplaces,

digital fraud platforms, and money-generating assets embedded in wider local and cross-border economies. ODI's 2023 briefing on trafficking for forced criminality and IOM's regional analyses both show that trafficking into scam compounds is organised through recognisable recruitment, transport, transfer, receipt, and exploitation stages rather than spontaneous ad hoc abuse.

The second distinction is legal and practical. Many trafficked workers in these compounds are forced to commit crimes. That means the issue is not exhausted by a simple labour-trafficking frame. It requires a forced criminality lens. OHCHR's earlier briefing paper on online scam operations and ASEAN's 2025 guidance on the non-punishment principle both reflect a growing recognition that trafficked people may be compelled into unlawful acts and should not automatically be treated as willing offenders. This matters enormously once rescues occur, because classification as "perpetrator" or "victim" can determine whether someone receives protection, detention, prosecution, or repatriation.

The third distinction is geographic. The public often imagines lawless jungle compounds detached from the wider economy. That is too crude. UNODC's work on casinos, underground banking, and organised crime shows that many criminal businesses in East and Southeast Asia have relocated into autonomous areas and special economic zones, where commercial infrastructure, weak oversight, and political ambiguity can converge. The "grey zone" problem is therefore not simple absence of the state. It is the presence of fragmented, selective, or compromised governance in locations attractive to both licit investment and illicit enterprise.

How the system actually works

Recruitment usually begins with deception, not overt kidnapping. INTERPOL, IOM, and OHCHR all describe false offers for jobs in customer service, tech support, marketing, hospitality, or online sales,

often advertised through social media, messaging apps, labour brokers, or informal migrant networks. The promise is straightforward: travel, accommodation, a better salary, and quick onboarding. That matters because it means prevention cannot focus only on border interception. The vulnerability often begins much earlier, at the point where economic aspiration meets digital recruitment.

Transport and transfer then convert deception into control. IOM's situation analysis describes several changes of hands between recruiters, transporters, facilitators, and compound operators. Victims may cross borders on apparently regular routes, sometimes with valid travel documents, before passports are confiscated or movements restricted. This is one reason the model is hard to spot early: the initial stages can resemble ordinary labour migration more than dramatic trafficking imagery. By the time coercion becomes unmistakable, the person is already in a controlled site, often in another jurisdiction.

Inside the compounds, exploitation is organised around productivity. OHCHR's 2026 report describes torture and other ill-treatment, sexual abuse and exploitation, forced abortions, food deprivation, and solitary confinement. INTERPOL adds debt bondage, extortion, and sexual violence. These are not incidental acts of cruelty. They serve a labour function. They create compliance in workplaces built around quotas, scripts, and fraud targets. In that sense, violence is not external to the business model. It is one of its management tools.

The fraud side is similarly systematised. Scam-centre activity includes romance-investment scams, impersonation fraud, crypto-related fraud, and other forms of digital social engineering. INTERPOL's broader financial-fraud assessment and UNODC's 2024 and 2025 work show that these operations increasingly rely on service layers beyond the compound itself: stolen data markets, underground banking, malware and scam-enabling tools, crypto laundering solutions, and more recently generative AI and deepfakes. This is important because it means the compound is only the visible labour site. The full system includes external providers that increase reach, efficiency, and adaptability.

That service-layer development is one of the clearest signs that the industry is maturing. UNODC said in October 2024 that Asian crime syndicates had integrated malware, generative AI, deepfakes, underground markets, and new cryptocurrency solutions into their operations. INTERPOL separately noted the use of AI to create convincing fake job advertisements that attract trafficking victims. The important point is not merely that criminals use new technology. It is that the sector is moving from crude fraud to modular criminal infrastructure, in which recruitment, coercion, deception, and laundering are all being professionalised.

Why these grey zones formed

They formed because certain environments offered a rare combination of ingredients: commercially usable land, permissive governance, strategic border location, access to electricity and digital infrastructure, and a political economy already comfortable with casinos, junkets, underground banking, and ambiguous capital. UNODC's 2024 casino report is especially helpful here. It argues that casinos, junkets, cryptocurrency, and underground banking have become critical components of organised-crime infrastructure in East and Southeast Asia, and that many connected businesses relocated into autonomous areas and special economic zones. Scam compounds did not emerge in a vacuum. They plugged into an ecosystem already designed to move money, attract opaque investment, and operate across blurred legal boundaries.

That explains why simple geographic descriptions are inadequate. A borderland compound is not important only because it is hard to reach. It is important because borderland and special-zone arrangements can complicate jurisdiction, dilute accountability, and create opportunities for parallel authority. When OHCHR reports allegations that border officials aided recruiters and that police were involved in threats and extortion, it is pointing to precisely this problem: victims are moving

through spaces where state and non-state power may coexist in ways that are difficult to disentangle. Such allegations should be treated carefully, but they matter because they show why the line between "criminal zone" and "regulated economy" is often unstable.

What most people still miss

The first thing many people miss is that rescue is not the same as resolution. Reuters reported in February and March 2025 that thousands of people pulled from compounds near Myawaddy were left in camps or holding sites awaiting screening and repatriation, with some unable to afford onward travel and others facing uncertainty over how authorities would classify them. AP described thousands of freed workers stuck in limbo. This matters because the trafficking story does not end when a person leaves the compound. In legal, humanitarian, and political terms, that is often when the next set of risks begins.

The second thing many people miss is that the industry survives crackdowns by moving faster than enforcement systems can coordinate. UNODC's 2025 "inflection point" analysis describes a spillover dynamic in which criminal groups relocate and adapt as pressure rises in one jurisdiction. Reuters reported in March 2025 that, even after multinational pressure, Thai police still estimated up to 100,000 people remained in scam hubs along the Thai-Myanmar border. Even if such field estimates should be treated cautiously, the broader point is clear: disruption of one site, or even one corridor, does not dismantle an industry built for mobility.

The third thing many people miss is that this is not merely a humanitarian crisis attached to cybercrime. It is also a governance and political-economy problem. ODI's work on scam-centre exploitation and broader political-economy conditions in Southeast Asia suggests that vulnerabilities are sustained by a mix of weak worker protection, migration pressures, debt, and institutional inconsistency. Put differently, the compounds are parasitic on existing fragilities. They do

not invent vulnerability from nothing. They monetise vulnerability that already exists.

Why this matters to leaders and donors

For leaders, the lesson is that human trafficking is adapting to the digital economy. The old mental model of trafficking, centred only on brothels, factories, or fishing vessels, is now too narrow. People can be trafficked into online workforces whose output is fraud against victims across the world. That makes this issue relevant not only to humanitarian actors but also to people concerned with digital trust, cross-border payments, migration systems, platform abuse, sanctions, and financial integrity.

For donors, the implication is that rescue-only thinking is insufficient. Protection, repatriation, and survivor support remain essential, but the system also depends on deceptive recruitment channels, permissive host environments, and laundering infrastructure. A donor strategy that funds only post-compound recovery may relieve harm without touching the architecture that regenerates it. A more serious philanthropic approach would ask which interventions affect recruitment, classification of victims, cross-border coordination, financial disruption, and legal safeguards against punishing trafficked offenders.

What meaningful intervention looks like

The first priority is correct legal and operational classification. If trafficked workers forced into scams are treated simply as fraud offenders, the system gains another layer of protection because victims become disposable and silence is reinforced. ASEAN's 2025 non-punishment guidance matters for exactly this reason. It is not a technical footnote. It is one of the legal mechanisms that can determine whether rescued people are protected, prosecuted, or lost back into the system.

The second priority is financial disruption. UNODC's recent reporting repeatedly emphasises underground banking, casinos, crypto channels,

and illicit online marketplaces as critical infrastructure for organised crime in the region. Sanctions actions by the UK and earlier coordinated measures by the UK and US show an emerging recognition that compound operators alone are not the whole target set. The service providers, marketplaces, facilitators, and laundering channels matter just as much.

The third priority is earlier prevention in the migration and recruitment chain. Because many victims are lured through apparently legitimate work offers, more scrutiny of online job recruitment, safer migration pathways, and targeted warning systems for at-risk populations are likely to matter more than generic awareness campaigns. IOM and The Mekong Club both point to exploitation of legal and irregular migration channels alike, which means the prevention challenge is not simply "stop illegal border crossings." It is "reduce the number of people who can be deceived into a coercive labour pipeline in the first place."

The fourth priority is realism about enforcement optics. Cambodia's new anti-scam law and recent crackdowns may prove meaningful, but AP's reporting also captures scepticism from experts who argue that shutting compounds without dismantling the surrounding protection and financial networks may not change the underlying economics enough. That scepticism is well founded. A visible raid is evidence of activity. It is not yet evidence of structural success.

Conclusion

The grey zones of Southeast Asia are not simply places where trafficking happens to coexist with online fraud. They are environments in which a new exploitation model has taken shape: one that converts labour deception into digital fraud, sustains productivity through coercion, launders proceeds through mature illicit-finance channels, and survives pressure by moving across permissive jurisdictions. That is why this issue deserves to be understood as a system, not a scandal.

The real test now is whether governments, donors, and institutions respond at the level the model actually operates. If they continue to intervene mainly at the point of rescue, or at the level of individual compounds, they will remain behind the problem. If they begin treating scam compounds as the labour sites of a larger criminal economy, the strategy changes. The task becomes not only freeing victims, but constraining the zones, channels, and financial architectures that make this form of trafficking profitable in the first place.

Methodology and source note

This briefing synthesises reporting, public records, policy research, and material from international organisations and government-linked sources available at the time of writing. It aims to distinguish clearly between verified facts, attributed allegations, estimates and analysis. Where evidence is evolving or public figures vary, that uncertainty is stated or implied conservatively. The phrase “grey zones” in this paper is an editorial framing used to describe permissive environments in which scam compounds and related criminal systems can thrive; it is not used here as a formal legal term.

Key sources

UNODC, Cyberfraud in the Mekong reaches inflection point, 21 April 2025.
OHCHR, UN report details grave abuses against those trafficked into scam centres, 20 February 2026.
INTERPOL, Human trafficking-fueled scam centres, June 2025.
OHCHR Bangkok, Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia, 2022 page summarising the briefing paper.
Reuters, UK sanctions Cambodia-based scam centre and crypto platform, 26 March 2026.
AP, Cambodia advances a scam center law with penalties of up to life in prison, 30 March 2026.
Reuters, Indonesia to question more than 500 citizens freed from Myanmar scam centres, 18 March 2025.
Reuters, Some foreigners pulled out of Myanmar scam centres face struggle to get home, 28 February 2025.
AP, They were forced to scam others worldwide. Now thousands are stuck in limbo, 9 March 2025.
ASEAN, Guideline on the Implementation of the Non-Punishment Principle for Protection of Victims of Trafficking in Persons, 2025.