



**GLOBAL
INITIATIVE**

AGAINST TRANSNATIONAL
ORGANIZED CRIME

MINIMIZING RISKS OF CRIMINAL EXPOSURE TO SCAM COMPOUNDS IN CORPORATE SUPPLY CHAINS

A GUIDE FOR REAL ESTATE
INVESTORS, DEVELOPERS AND
CONSTRUCTION CONTRACTORS

Lindsey Kennedy | Nathan Paul Southern

DECEMBER 2025

ACKNOWLEDGEMENTS

The authors would like to thank the Government of Norway for supporting the research and publication of this policy brief.

ABOUT THE AUTHORS

Lindsey Kennedy is an investigative journalist and research director at The Eyewitness Project, which specializes in the overlaps between organized crime, conflict and corruption. Her work focuses on cyber scam operations, human trafficking, illicit commodity flows and environmental crime, and has been featured in *Foreign Policy*, *The Guardian*, HuffPost, Al Jazeera, *The Sydney Morning Herald* and NPR. She has co-authored Global Initiative Against Transnational Organized Crime (GI-TOC) reports on trafficking in the Mekong region.

Nathan Paul Southern is a non-traditional security specialist, director of operations at The Eyewitness Project and PhD candidate in international relations at the University of St Andrews. He specializes in the overlaps between conflict, organized crime and corruption, and has consulted on reports for the Brookings Institution, the GI-TOC and the Institute for Integrated Transitions, and written for Al Jazeera, *Foreign Policy*, HuffPost and the *South China Morning Post*.

© 2025 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted
in any form or by any means without permission in writing from
the Global Initiative.

Cover: © Sebastian Kahnert/picture alliance via Getty Images

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

CONTENTS

Acronyms and abbreviations	2
Summary.....	3
Key points.....	4
Introduction	5
The enablers: an overview	8
Real estate developers.....	8
Construction contractors.....	9
Funding bodies and development banks.....	11
What are businesses doing to stay clean?	13
A practical guide to identifying and tackling risks?	16
Courting funding and partners	17
Marketing and promotional materials.....	18
Securing permissions.....	19
Selecting construction contractors	19
Appendix 1: Case study: Yunnan Jincheng and Dong Lecheng	20
Appendix 2: Unknowable customers? Barriers to effective background checks	22
Notes	24

ACRONYMS AND ABBREVIATIONS

ADB	Asian Development Bank
ASEAN	Association of Southeast Asian Nations
BRI	Belt and Road Initiative
GTSEZ	Golden Triangle Special Economic Zone
KYC	Know your customer
RFA	Radio Free Asia
SEZ	Special economic zone
SOE	State-owned enterprise



SUMMARY

Highly organized cyber fraud in South East Asia is widely run from so-called scam compounds, which are purpose-built or modified buildings that meet the precise requirements of this criminal industry. The compounds provide crucial infrastructure for various forms of online scams, fraud and other cybercrime.

Often appearing to follow a similar blueprint,¹ these buildings are at the epicentre of a global criminal industry. They house hundreds – and sometimes thousands – of people, many of whom are held captive and forced to cheat or extort unsuspecting victims around the world.

Previous research and analysis on cyber scam operations in the region has focused predominantly on one of the following aspects: criminal groups, their direct institutional partners, financial architecture, infrastructure and communications. Largely missing from the picture, however, are the myriad industries and suppliers that interact directly with scam compounds and companies in their physical location, and whose activities are not necessarily criminal in themselves but are instrumental in keeping the criminal industry alive.

This policy brief focuses on the pre-operational phase of cyber scam compounds, making it particularly relevant to private investors, multilateral development banks, developers, real estate companies and construction companies. It describes how these entities contribute to and facilitate – or are at risk of contributing to and facilitating – criminally funded or exposed development projects that host cyber scam operations.

This is the first in a two-part series on how organizations can avoid buying from, selling to or partnering with criminal actors in the cyber scam space. In the second policy brief, we will look at how companies that are (or are considering becoming) suppliers or partners to existing developments can recognize red flags and respond appropriately.

This first policy brief provides practical guidelines that companies can follow to avoid entering commercial relationships with cyber scam operators. It empowers them to strengthen know your customer (KYC) strategies and background checks, better identify threats and vulnerabilities and successfully distance themselves from criminally exposed ventures before it becomes too difficult to disentangle their business interests.

This policy brief draws on extensive data collected through field research in Cambodia, Laos and Thailand (at the border with Myanmar) from 2023 to 2025. It was triangulated with available literature and media reporting.

Key points

- There appears to be a spectrum of complicity of private sector companies, ranging from those that are aware and actively driving and profiting from cyber scam operations to those that are unaware of how their activities may be benefiting these criminal operations.
- Scam compound hubs frequently follow the same development trajectory, meaning potential partners can feasibly identify warning signs to distance themselves accordingly. However, the earlier they identify these red flags, the better placed they will be to protect their business against criminal exposure.
- Actors driving forwards large-scale development projects that are later found to house scams and forced criminality sometimes have a history of criminal activity or exposure that is documented in the public domain and can be uncovered through rigorous background checks. This underlines the need for compliance and KYC procedures in all relevant industries.



INTRODUCTION

Cyber scam operations are proliferating, defrauding victims at ever greater scale. Cryptocurrency revenue from online scams increases by an average of 24% year-on-year,² and according to the Global Anti-Scam Alliance, victims lose over US\$1 trillion to online scams annually.³ Bearing in mind that the entire world's combined GDP is currently around US\$110 trillion,⁴ this means nearly 1% of the world's wealth is transferred from individuals to criminal organizations every year, solely through scams.

Factoring in the total cost of cybercrime to businesses, overall losses are expected to hit US\$10.29 trillion dollars in 2025 alone.⁵ This includes money stolen directly by hackers, ransomware, and phishing, but also the financial burden of dealing with these threats.

Successful scams are financially and psychologically devastating to victims. They pose serious economic and security threats both to nations targeted by scammers and to those hosting criminal groups that enrich and empower themselves through these activities. The scam industry also constitutes a hugely lucrative arena for investors and suppliers.

In South East Asia, industrial-scale cyber fraud is particularly concentrated in Cambodia, Laos and Myanmar. There, some remote communities may even have gained access to basic services, utilities and road networks through their proximity to scam compounds, since the owners of these enterprises are influential enough to direct infrastructure development decisions⁶ or directly fund such development,⁷ potentially as a precondition for government approval.

Many (although not all) scam compounds have distinctive features that help identify them on sight, including from satellite imagery when complete. However, there are often also clear signs during the design and construction phases. Red flags therefore emerge long before these compounds become operational.

Understanding why certain elements are critical to scam operations can also help identify scam centres that are modified, disguised as or form part of other kinds of buildings (e.g. casinos, warehouses and hospitals). However, for simplicity, this report specifically discusses the widely replicated model of purpose-built compounds, where form clearly follows function and identifiable features are in plain sight.



Cyber scam compounds have proliferated in parts of South East Asia. Their construction and operations rely on a supply chain of private sector companies. *Photo: GI-TOC*

In South East Asia, a long and growing list of known compounds replicate this model across a range of environments. Compounds appear in capital cities, small towns, mountain villages, beachfront developments, technology parks, special economic zones (SEZs) and at border crossings.

The common thread between their chosen locations is that criminal networks can run their operations securely – protected from intervention and interrogation by the authorities. This includes exercising full control over their workforces, especially when those workers have been trafficked and coerced into their roles.

The compounds do not build themselves. For a project of this nature to go ahead, a chain of developers, investors and construction contractors need to sign off on plans, architectural drawings and building specifications, among other things. As we discuss in this report, developers of cyber scam compounds typically source foreign direct investment and implementing partners from overseas.

They may also seek funding from development banks and foreign governments, try to integrate themselves into China's genuine Belt and Road Initiative (BRI) projects, or more often feign a connection to the BRI to mislead potential investors. They need construction partners and contractors to build purpose-designed locations, or real estate companies that understand what they do and are willing to lease them the right kind of space for their operations.

The compounds are also not self-sufficient entities. They need reliable electricity and high-speed internet. They need transportation infrastructure and the means to deliver workers, trafficked or otherwise, to their doorstep. They need food, water, computers, smartphones, international SIM

cards, multi-port charging stations, office furniture, bunkbeds, reinforced doors and robust locks for keycard-only entry. These compounds also incorporate nightclubs and karaoke bars, where sex workers reward compliance and entertain workers permitted to leave their building on rare days off.

Some associated entities exist in a legal and/or ethical grey area, fully aware of the nature of the businesses they interact with. In some cases, they have adapted proactively to tackle the niche requirements of this lucrative target market. Others may be oblivious to the role they play in the industry – or, if they do harbour suspicions, do not consider themselves responsible for how their products and services are used, or simply feel ill-equipped or too powerless to disengage from this criminal industry (or counter it).

This can lead to varying degrees of complicity, corruption and criminality, both by domestic companies and by foreign partners. While some entities might be oblivious to their criminal exposure, they may be opening themselves up to a broad range of risks nonetheless.



THE ENABLERS: AN OVERVIEW

This section takes a closer look at the roles played by real estate developers, investors and construction companies in the development of scam compounds and forced online criminality hubs.

Other exposed entities are firms typically subcontracted by these actors for specific or specialist requirements, including architecture firms and interior designers, as well as companies hired to install electricity and plumbing, test safety features, provide construction equipment and materials, and so on. Their touchpoints and the red flags they should look out for are broadly the same.

Generally speaking, risks can arise from any kind of real estate project that could be repurposed as a scam compound, such as apartment buildings, hotels, mixed-use office space and accommodation buildings. However, investors, developers and construction contractors considering involvement in any SEZ, casino or online gambling-related project should exercise additional caution and conduct rigorous risk analyses, as casinos in South East Asia are known to be highly criminogenic.⁸

Attempts to facilitate a legal offshore online gambling industry in Cambodia and the Philippines were overwhelmed rapidly by violent organized crime groups,⁹ laying the foundations for the regional cyber scam crisis.¹⁰ This led both countries to reinstate a blanket ban on online gambling.¹¹ Online gambling is also illegal in Laos (with the exception of SEZs) and Myanmar but remains widespread.¹²

Real estate developers

Developers of scam compounds are often adept at hiding out in the open – if, indeed, they hide at all. They have trumpeted major new real estate developments, SEZs and entire satellite cities that have later been revealed to house cyber scam operations.¹³

Involvement in the creation and development of casinos, SEZs and tourist facilities that incorporate casinos and/or online gambling infrastructure has provided a route for criminal actors to gain a foothold in poorly regulated countries in South East Asia.¹⁴ This laid the groundwork for the proliferation of scam compound hubs across the region.¹⁵ Appendix 1 to this policy brief includes a case study of an individual and associated entities with track records as core participants in the scam compounds industry.

Research has shown that that scam compound developers frequently claim or insinuate (often falsely) that their projects are backed by government actors, funding or initiatives, especially in relation to the BRI.¹⁶ The BRI is especially vulnerable to abuse because there is no central system or reporting in place that external actors can use to verify such claims.

This makes it easy for any developer to say they are ‘actively responding to the BRI’ (the standard phrase used by BRI partners). There is little scope for potential partners to prove otherwise, unless China publicly contradicts this.

Moreover, the complexity of large-scale BRI projects, which can be compartmentalized and subcontracted out to companies that are less carefully vetted, means that a real estate development may be vulnerable to criminal contamination even if it is genuinely linked to a BRI project.

A striking example is She Zhijiang,¹⁷ who spearheaded Shwe Kokko (Yatai New City) in Myanmar.¹⁸ According to local media reports, She Zhijiang is said to have marketed Shwe Kokko as a BRI project until the Chinese embassy in Yangon denied any link.¹⁹ Actively fabricating a connection to the BRI (or making any misleading claims about funding sources) is a clear red flag.

However, even when a project is genuinely linked to a development funded by reputable sources, caution must still be exercised. A BBC report revealed that Dara Sakor, a US-sanctioned development that houses several sites identified as scam compounds, including Long Bay, was featured in Beijing’s official BRI yearbook.²⁰ Tianjin Union Development Group, the developer of Dara Sakor, benefited from a US\$15 million BRI bond from the China Development Bank in 2017.²¹

Failure to carefully vet, verify and assess developers’ claims, or to continue contracts when such claims prove to be false, can expose potential partners to criminal, reputational and financial risk. This is especially so in cases where projects have provable links to politically exposed persons, elites and government programmes.

Construction contractors

Scam compound operators require companies to construct buildings and infrastructure, and in some cases recruit reputable private or even foreign state-owned enterprises (SOEs) to construct scam locations.²² Some contractors may be unaware of the ultimate purpose of these projects, but others appear to work willingly with (or close to) sites that are notorious for human trafficking and forced labour.

For example, during a trip to the Mae Sot/Moei River area of Thailand in November 2024, two independent researchers noted the presence of concrete mixers branded KK Concrete (see the photo). The name bears a striking similarity to KK Park, a cybercrime hub housing scam compounds across the border in Myawaddy, Myanmar.²³

Photos and locations in the authors’ possession show trucks transporting pre-mixed concrete from the Thai side of the border towards, or potentially into, KK Park.²⁴ After a researcher publicly alleged that KK Concrete was supplying concrete for the expansion of scam compound facilities,²⁵ a subsequent trip in March 2025 revealed that the mixers on the Thai side of the border had been dismantled.²⁶ It appeared that the KK Concrete factory had relocated into Myanmar’s territory.²⁷ However, a Thai company of the same name still advertises its headquarters as Mae Sot,²⁸ with delivery to Myawaddy.²⁹



A KK-branded truck drives in the direction of KK Park, a scam compound hub in Myanmar, March 2025. *Photo: Cezary Podkul*

There are often early-warning signs that point to the construction of a scam compound, even if the project is ostensibly commissioned as a casino, hotel or other form of entertainment venue. Major warning signs will include extensive dormitories, or initial plans being updated to house a far higher density of people in each room than the original floorplan would accommodate.

Requests for security features or blackout rooms or floors that would have little logical purpose beyond controlling or intimidating people trapped inside would need to be made early on. These features are consistent with scam compound operations.

In the earliest stages of a project, developers of sites that are billed as casinos, tourism hubs or business parks but later turn out to be scam compounds are frequently implicated in human rights abuses and land disputes with surrounding communities.³⁰ Such developers are often accused of failing to meet legal or ethical obligations centring on transparency and local participation or consultations.³¹



A KK Concrete production facility on the Thai side of the Moei River, close to the scam compounds in KK Park, November 2024. *Photo: Cezary Podkul*

In some cases, alleged abuses are so severe that developers are designated for international sanctions. Notable examples include M.D.S Henghe Thma Da SEZ and Dara Sakor in Cambodia, and the Golden Triangle Special Economic Zone (GTSEZ) in Laos. Developers of all three sites were subject to sanctions long before it became clear that they housed scam compounds.³²

While cases of labour exploitation, rights violations and even human trafficking in the construction industry are certainly not limited to scam compound developments, failure to demand accountability for these abuses by development partners and funders helps entrench criminality and corruption in the sector. This allows actors to operate with impunity and fosters conditions in which the scam industry can flourish.

Many migrant construction workers face similar patterns of abuse to scam workers during recruitment and employment.³³ As such, failure to implement comprehensive anti-human trafficking policies that address these vulnerabilities early on risks establishing a culture where breaching workers' legal rights or even engaging in trafficking and exploitation onsite goes unchallenged – potentially laying the groundwork for other forms of criminality and abuse.

Hundreds of Chinese workers were reported to be working illegally on construction sites in the Myanmar Yatai Shwe Kokko SEZ in 2019,³⁴ while in Cambodia, unsafe and exploitative practices affecting both Chinese³⁵ and Cambodian workers³⁶ on construction sites in prominent online gambling and scam compound hubs like Sihanoukville³⁷ and Chrey Thum (Kandal, Cambodia)³⁸ have been linked to fatal building collapses³⁹ and other tragedies.⁴⁰ This has resulted in prison sentences for some of the Chinese and Vietnamese construction contractors and managers deemed responsible.⁴¹

Funding bodies and development banks

The World Bank, Asian Development Bank (ADB) and other international development banks perform significant due diligence on SOEs and private companies that bid for contracts they are funding. This includes looking for evidence of bribe payments, undeclared conflicts of interest, fabricated credentials and other dishonest or corrupt practices that may be used both during the bid stage and once a project is underway. Entities found to be in breach of these rules are blacklisted from bidding for other projects either for a set period or indefinitely, depending on the severity of the breach or whether the company has past infractions. The major development banks also collaborate on cross-debarment, meaning that a sanction decision made by one organization will be upheld by others in the group.

However, while most of these organizations publish the rationale for their decisions, the ADB rarely makes public why a company has been debarred. Once a company is removed from the list, it can be hard to find any record of their debarment, still less the rationale. This limits KYC and risk assessment efforts by future partners.

As of 10 February 2025, there were 1 285 companies on the World Bank's debarred list, including cross-debarments (340 from the ADB) and subsidiaries of sanctioned entities. Strikingly, some of these companies were able to continue operations uninhibited after being added to the list – and without attracting condemnation or criticism from relevant government backers.

For example, the World Bank listed 349 Chinese entities and individuals as sanctioned or debarred from procurement processes due to corrupt, fraudulent or prohibited business practices,⁴² but few appear to have suffered any repercussions in China. This includes one company headquartered in Hong Kong, which was flagged by the ADB in July 2024 for fraud, but maintains active branches in several countries. An investigation by the ADB's Office of Anti-Corruption and Integrity found that the company fraudulently presented itself as eligible to participate in an ADB-funded contract despite having been debarred by the ADB. However, as the ADB does not publish the rationale for debarments as standard, it may have been difficult for partners to assess the level of risk or make judgment calls on the contractor's integrity. (It should be noted that there is no indication that this particular company has actively constructed scam compounds.)

Even when the reasons for debarment are known, developers hand lucrative contracts to construction contractors with criminal histories and associations. Another state-owned Chinese construction enterprise was blacklisted for bribery by the Bangladesh government in 2018⁴³ and added to ADB's sanctions list in 2021.⁴⁴ That same year, it won a Cambodian contract worth US\$308 million dollars. Voice of Democracy reported that the firm was tasked with 'reclaiming' hundreds of hectares of Cambodian coastline by filling a pristine bay with sand in a supposedly protected area without having performed an environmental impact assessment.⁴⁵

This was part of the US\$16 billion Ream City project⁴⁶ (later reamed Bay of Lights) developed by Prince Holding Group⁴⁷ through its subsidiary, Canopy Sands.⁴⁸ In October 2025, the group, its founder and hundreds of related companies (including Canopy Sands) were sanctioned by the US government and subjected to over US\$15 billion in asset seizures. South Korea issued similar sanctions the following months.⁴⁹

The US alleged that the Prince Group operated Cambodian scam compounds and transnational illegal gambling operations linked to human trafficking and torture, and had laundered billions of dollars in illicit funds.⁵⁰ This followed years of reporting on Prince Group's activities by researchers,⁵¹ NGOs⁵² and investigative journalists.⁵³ Chinese court documents from 2022 accuse the company of recruiting illegal gambling and money laundering operators from China since at least 2016.⁵⁴

Even when a bid does not technically fall foul of the rules set by multilateral development banks, these organizations may still make questionable funding decisions in areas at high risk of scam compound proliferation. For example, the ADB green-lit US\$250 million in loans for Chinese-led, cross-border infrastructure development projects between Lincang (China) and Chinshwehaw (Myanmar) as part of the Yunnan Lincang Border Economic Cooperation Zone Development Project. This came at the height of scam industry expansion in the area, without the bank appearing to acknowledge the elevated risks.⁵⁵



WHAT ARE BUSINESSES DOING TO STAY CLEAN?

A major driver of companies putting in place anti-corruption and risk management policies is whether they are legally obliged to do so by their own government or their host government. Various governments have taken steps to pressure companies into taking responsibility for complicity in corruption and criminal behaviour, including by partners and suppliers (see 'Degrees of complicity').

However, in countries that are members of the Association of Southeast Asian Nations (ASEAN), a common reason cited for not assessing and managing these risks is that doing so is not mandatory.⁵⁶ In 2020, only 55% of companies domiciled in the ASEAN region and surveyed by the Organization of Economic Cooperation and Development had any written policy in place governing ethics. Meanwhile, 53% maintained responsible business practices and only 46% carried out social or environmental risk assessments as part of their due diligence on direct suppliers or business partners.⁵⁷

Only one in five companies extended these risk assessments beyond the first tier, i.e. the broader supply chain.⁵⁸ Of the companies that had risk management policies in place, nearly two-thirds (65%) took into account breaches of human rights by suppliers/partners, while 28% said they had a policy that compelled them to investigate internal rights breaches.⁵⁹

For local or regional companies focused on meeting their own country's laws and regulations, supplying or entering into a joint venture with a foreign investor from a jurisdiction where anti-slavery legislation is more stringent may mean accommodating onerous new sets of regulations, which may be met with resistance.⁶⁰ Moreover, international companies are prone to exercising these demands inconsistently, often in response to a particular complaint, report or flurry of media attention focusing on their link to unethical practices.⁶¹ It is easy to see how this can catch local partners off guard and shift responsibility to them for solving a long-running, systemic, poorly documented problem in an unrealistic timeframe. Avoiding or seriously tackling the problem should have been built into the foreign partner's development strategy, risk assessments and profit forecasting from the outset.



A view of the Kings Romans Casino in Laos. As part of their due diligence, funders and partners should ascertain whether a construction project is located at a scam hub. © Sebastian Kahnert/picture alliance via Getty Images

Perhaps most importantly, analysis of downstream supply chain risk and analysis of upstream risk appear to be viewed as largely different problems. None of the organizations consulted for this report had received requests by their clients to investigate instances of human trafficking and slavery, for example as part of KYC processes and due diligence. In other words, even when companies are motivated to investigate human trafficking downstream in their supply chains, they seem less concerned with whether it is happening further upstream, despite profits generated from human trafficking and related criminal activity by their clients putting them at direct risk of receiving illicit funds and engaging in money laundering.

Degrees of complicity

It may be helpful to consider actors involved in the pre-operational/development stage of a scam compound in terms of where they fall on a spectrum of awareness and complicity, as visualized in Figure 1. From left to right, this spectrum ranges from companies that appear to be:

- **Unknowingly complicit:** Companies that could feasibly be in the dark about the project's criminal exposure and/or have been misled about its intended use.
- **Unwillingly complicit:** Companies that are likely to have begun to understand or suspect the risks but feel it is too late or complicated to pull out. Entities on this part of the spectrum may want to distance themselves but are daunted by the obstacles or potential repercussions.
- **Passively complicit:** Companies that can reasonably be expected to recognize red flags or to be aware of the criminal reputation of the developer they are working with, but do not appear to feel compelled to distance themselves, whether out of indifference, convenience or because they do not feel it is their responsibility to raise the alarm.

- **Actively complicit:** Private sector or even state-owned actors that show signs of being willing, enthusiastic participants and are contracted by the primary developer/compound owner. This may refer to any entity that joined the project knowing it would be used as a scam compound and chose to pursue this lucrative opportunity, but especially those that tailor their services or design to suit the needs of scam compounds. This category includes companies that specialize in serving the scam compound niche and those whose portfolio includes both grey market and 'normal' real estate projects.
- **Direct participants:** These are companies directly controlled or created by the criminal actors that sit at the heart of the project, including as front companies, with the express purpose of building, managing and operating the project(s) that will be used as a scam compound, or disguising/laundering funding sources (they may be fronted by someone else to conceal this direct relationship with scam developers). As with actively complicit contractors, some may exist exclusively to build these compounds while others may be 'bridge' companies, i.e. they also invest in non-scam-compound or mixed-use real estate, or have portfolios in unrelated sectors, helping them to maintain an image of legitimacy and to commingle licit and illicit income streams for money laundering purposes. This model is particularly insidious as it can be very difficult for potential partners to spot red flags if the company also has an apparently legitimate portfolio. Partners may engage with seemingly credible projects without realizing they are at risk of enabling a criminal enterprise to cash out laundered funds. This also helps criminal enterprises to gain a foothold in the licit economy, entrenching their influence and making them harder to dislodge.

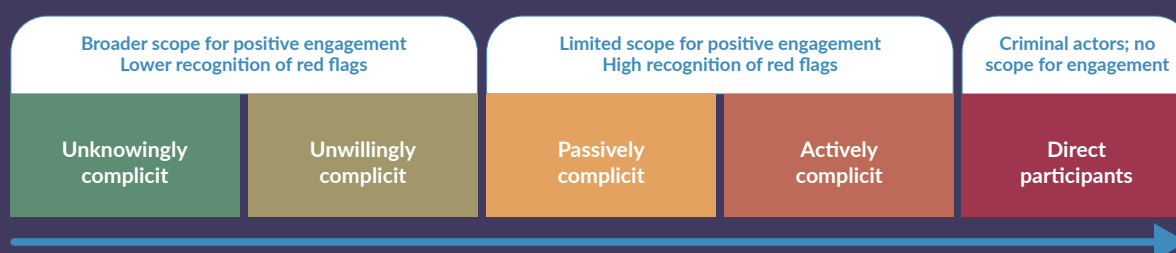



FIGURE 1 Spectrum of complicity for entities involved in the funding, development or construction of scam compounds.

NOTE: These categories are not rigid and the role of companies may change over time.

Analyzing where an entity may fall on this spectrum can help to assess their degree of accountability and culpability. It also helps to identify potential routes for engagement and collaboration. For example, an entity that has little idea of the impact of its criminal exposure may benefit from toolkits to help it identify red flags early on. Companies that are already embedded and concerned about the implications of this may benefit from support in blowing the whistle and extricating themselves from partnerships. At the other end of the scale, where ethical considerations are less persuasive, fear of reputational and financial harms from fines may be more effective. The very worst offenders are unlikely to respond to interventions that do not lean on regulatory action or criminal proceedings. ■



A PRACTICAL GUIDE TO IDENTIFYING AND TACKLING RISKS

The severity and magnitude of the crimes perpetrated by criminal actors in the cyber scam industry is staggering, ranging from tens of billions of dollars in theft to money laundering, sanctions evasion, human trafficking and sexual exploitation.

Entities that fail to invest sufficiently in KYC checks that go beyond the bare minimum may later find it difficult to distance themselves from or exit these agreements. They also risk legal, financial and reputational consequences if they are deemed to have been complicit in crimes.

Such companies are particularly vulnerable if pressurized host governments decide to scapegoat them for these criminal activities, or if cases are brought against them in other jurisdictions that have stringent rules on corruption, bribery or handling criminal proceeds.

For unknowing or unwilling participants, simply being made aware of the criminal exposure risk and the red flags involved may suffice as a catalyst for adapting and updating internal policies to minimize the risk of exposure. Entities in this category offer the most potential for productive dialogue and collaboration in efforts to tackle the forced cyber fraud industry.

The recommendations below primarily target entities that do not yet know, or may have begun to suspect, that their projects or partners are at risk of criminal exposure in the scam industry – and want to ensure that they do not become complicit. These steps are crucial for local and international partners alike.



Construction at Dara Sakor, a US-sanctioned development that houses several sites identified as scam compounds. Such projects may run the risk of being exploited by scam compound investors. © Artur Widak/NurPhoto via Getty Images

Courting funding and partners

Potential partners and investors who are not yet implicated in a project have a key role to play in vetting their partners and requesting extensive information and documentation to demonstrate the project's validity.

Potential funders and partners should ascertain or be on the lookout for:

- 1. Whether the construction project is located at a known scam location.** This applies to any area where a high density of scam compounds has been reported. While a large city will contain other legitimate industries, any project in a town, village, SEZ or industrial park that is already dominated by scam compounds with little to no significant legitimate economy should be an automatic red flag. This is especially so if the developers do not acknowledge this reality or explain how they plan to pivot away from it.
- 2. Adverse media coverage, research reports, sanctions decisions or lawsuits that indicate the company or key actors involved in the project have a history of criminal or corrupt practices.** Even a basic internet search may reveal serious red flags, including reports of open criminal investigations or arrests. (Note that even if the lead developer has registered a new company or joint venture in a country that does not list directors and shareholders in publicly available corporate records, the developer or any law/accountancy firm it has appointed as an intermediary should be able to provide these details).
- 3. Whether the project developers or their business associates have registered gambling-related companies or cryptocurrency trading platforms, either in the host country or elsewhere, or have applied for gambling licences, especially in offshore locations like Cyprus or Curaçao.** Even if in-person gambling is legal in the host country and/or the development includes a physical casino, promoting offshore online gambling sites is often illegal. Connections to international

online gambling networks thus put potential investors and partners at high risk of criminal exposure or money laundering. At a minimum, this should trigger enhanced due diligence checks and risk assessments.

4. **Whether any investors or key personnel linked to the project have acquired citizenship by investment or purchased a 'golden passport', especially if they changed their legal name in the process.** There may be legitimate reasons for doing so, but if so, it is reasonable to ascertain why. While this information is not always made public, some countries publish the names of individuals that acquire citizenship by investment, for example in royal gazettes. Acquisitions of citizenship may also be cited in media reports, government/company press releases or old social media posts. These potential partners may have used their golden passports as official identification when registering companies in publicly available registers or when signing other documentation submitted during contract negotiations.

Marketing and promotional materials

Developers of any ambitious real estate project or SEZ will naturally present their concept in the most exciting light. This is a pivotal moment when criminal actors involved in cyber scam operations have previously provided clues about the direction of the project or their trustworthiness.

For example, marketing materials for the Yatai development in Shwe Kokko, Myanmar, inadvertently displayed Chinese investor She Zhijiang's real name (and revealed other Chinese investors),⁶² exposing his transnational criminal background.⁶³ Additionally, publicity photos highlighted his relationships with political and military leaders,⁶⁴ some of whom were later sanctioned alongside She Zhijiang for their roles in facilitating human trafficking for forced criminality.⁶⁵ In Cambodia, a video promoting early plans for Dara Sakor⁶⁶ presented this as part of the same network as the Kings Romans casino, an entity in the GTSEZ in Laos that was sanctioned.

While barriers to effective background checks have increased (see Appendix 2), as part of KYC efforts, potential partners should:

- Scan promotional materials carefully for information that contradicts official proposals or the stated purpose of the development.
- Check these promotional materials carefully for images of or references to criminal actors, online gambling industry figures, or members of military groups or politically exposed persons.
- Ascertain whether there is any positive independent media coverage of the project (i.e. that was not paid for by the developers or government backers).
- Cross-reference this against negative coverage or NGO reports on land grabs and other potentially abusive, corrupt or criminal activity.
- Avoid allowing their logo or photos of high-level staff to be used to promote the project before they are officially involved in it and be sceptical of social media posts or promotional materials that feature other high-profile individuals without clarifying their relationship to the project.

Securing permissions

Once funded, project developers usually need local authorities to sign off a leasehold or freehold agreement and resolve any potential land disputes. In jurisdictions where corruption is prevalent, this creates significant risk exposure to bribe-seeking, cronyism and related money laundering risks.

Potential partners should:

- Ensure that all legal requirements such as environmental impact assessments are completed in accordance with laws, even if told by partners that they have acquired an exemption.
- Take seriously potential conflicts such as land rights or environmental damage to protected land; community violence and other illicit activities such as illegal logging may be early warning signs of criminal contagion.
- Demand transparency to guard against corruption and bribery (and refuse to pay bribes).

Selecting construction contractors

How construction contracts are framed will depend on the type of development. For example, if funded with loans through the BRI, it will be awarded to a Chinese SOE. However, depending on the size of the project, smaller construction firms may be chosen that have experience in building purpose-designed scam centres. There is also a high risk of cronyism in the selection of suppliers for lucrative construction projects.

Partners and funders should:

- Demand transparency in the bidding system and refuse to pay bribes.
- Ensure that the selected construction company has anti-human trafficking policies and fair working conditions in place, especially for migrant workers (or, in the case of construction contractors, have implemented these policies themselves).
- Ensure that neither the developer nor the construction company has been hired to build any other locations alleged to house scams or forced criminality.
- Flag and demand explanations for any alterations to original plans or completed real estate projects that appear to change the intended purpose by excessively securing the building, preventing people leaving or drastically limiting points of access and exit, or that are clearly designed to house a far larger workforce than could feasibly be employed in the immediate vicinity. Common features installed at scam compounds include anti-jump nets, keycard-only access to public areas, barred balconies, blacked out windows and areas designed to be entirely self-sufficient behind high walls and gates.
- Publish and make accessible the rationale for debarring companies as well as a list of companies that have previously been debarred.



APPENDIX 1

CASE STUDY: YUNNAN JINCHENG AND DONG LECHENG

Some companies that are actively involved in developing scam compounds have long histories of criminal exposure that should have been major red flags for potential partners, co-investors and construction contractors. For example, one company sanctioned in perpetuity by the World Bank is Yunnan Jincheng Construction Engineering Co., Ltd, which became subject to sanctions in March 2020. Available information suggests that the company did not contest the sanctions proceedings.⁶⁷

This debarment stemmed from a fraudulent bid for a water supply construction project in Zhejiang, China.⁶⁸ The Yunnan Jincheng group is owned by Dong Lecheng, who was sanctioned by the UK government in December 2023⁶⁹ and the US government in September 2025⁷⁰ for running criminal cyber scam compounds in Cambodia, where he acquired a passport and changed his name. He had been previously convicted of money laundering in China in 2008 and has been investigated for bribery.⁷¹


Dong Lecheng admitted in a statement in 2022 that Yunnan Jincheng developed the Jinshui Park real estate project in Sihanoukville, which has been implicated in 'cyber slavery',⁷² although he claimed to have sold the building to an undisclosed buyer by the end of 2018.⁷³ Previously, he claimed that Jinshui Park (and a casino hotel/scam compound development on Otres Beach)⁷⁴ aimed to 'implement the BRI and promote the joint development of the aviation tourism industry'.⁷⁵ Photos of the construction site for the development project containing Jinshui Park⁷⁶ show that these plans were reportedly part of a site⁷⁷ encompassing multiple real estate projects, including Golden Sun Sky⁷⁸ and the adjacent KBX Hotel.⁷⁹ Signage in these photos indicates that the construction contractor was Yunnan Construction International Holdings, a Chinese SOE.

In November 2020 – eight months after Dong Lecheng's company was blacklisted from bidding for investment projects funded by multilateral development banks – he presided over the grand opening of Ruili Bank of Cambodia, alongside the governor of the country's national bank. The Yunnan Jincheng website posted a statement saying it had invested in the bank to further Chinese government investment interests in the country by helping Cambodia integrate with the BRI.⁸⁰ There is, however, no evidence to suggest that any of Dong Lecheng's activities and investments had a genuine link to the BRI.

A comprehensive background check on Dong Lecheng and his companies would have highlighted publicly available information that should have raised major red flags for potential investors and partners. For example, he was found guilty of facilitating cross-border illegal gambling through his flagship hotel in China 2008⁸¹ and was accused of laundering over a billion dollars through the same hotel.⁸² Academic research published in 2018 described the corporate dealings strategy of Dong's Jingcheng Group in China's Yunnan province as 'a remarkable case of institutional capture' and 'political elite-business elite symbiosis'.⁸³

Given that Dong Lecheng claimed to have won a 75–90% share of construction contracts in the Chinese city of Ruili (worth approximately US\$3billion),⁸⁴ it seems reasonable that an investor of this profile would normally see his name and status as an asset when expanding into new markets. The timing of his decision to relocate to Cambodia in 2014 – at the peak of Chinese President Xi Jinping's nationwide corruption crackdown – and to acquire a new citizenship and identity (Cambodian royal decrees show he changed his legal name to Heng Tong) should therefore have prompted questions. He was eventually placed on financial and travel sanctions lists by the UK in December 2023 and the US in September 2025 for his alleged role in facilitating human trafficking into Cambodian scam compounds.⁸⁵ However, records in Cambodia's corporate registry show that he remains a listed director of various Cambodian companies.

While Dong Lecheng's marketing campaign may have appeared persuasive to potential partners at first glance, a thorough KYC strategy would have swiftly exposed red flags. This illustrates multiple avoidable failings both by the government officials who green-lit his projects and by his construction and investment partners. Distinguishing between negligence and complicity is a controversial debate. However, basic safeguarding failures by these partners must be subjected to greater scrutiny, accountability and penalization when projects they profit from are shown to be criminally exposed in a context where this outcome could reasonably have been predicted.



APPENDIX 2

UNKNOWABLE CUSTOMERS? BARRIERS TO EFFECTIVE BACKGROUND CHECKS

Developers of real estate projects that are designated or later utilized as sites for scams, illegal gambling, forced criminality or other kinds of exploitation often go to great lengths to promote these projects as legitimate. Such promotion indicates that these partners are entirely unaware of the true nature of the business they are engaging with until the relationship has already been publicized and contracts signed. Once in place, it becomes highly complex from a legal, reputational or even safety perspective to exit an arrangement. It becomes especially dangerous if the owners of the compound act with impunity and benefit from government protection.

Images of visits or meetings with political figures might initially have been taken by a prospective partner as a stamp of legitimacy. For example, in February 2024, the GTSEZ and Kings Romans casino in Laos publicized a visit by the German ambassador to Laos,⁸⁶ presenting this as an official delegation. The GTSEZ, Kings Romans and their owners are sanctioned by the US⁸⁷ and UK⁸⁸ governments for alleged crimes ranging from trafficking children into sex work to facilitating forced labour at scam compounds. The German embassy in Laos appears not to have contradicted or commented on the GTSEZ's narrative, at least not publicly, even after a leading cyber scam research organization published details of the visit online.⁸⁹ Later that year, owner Zhao Wei received a national development award from the Laos government,⁹⁰ gaining positive coverage in state-linked media in Laos and China.⁹¹

This kind of messaging can make it difficult to run accurate background checks, especially given that many countries where politically protected cyber scam operations are rampant also perform poorly in terms of freedom of expression and press freedom.⁹² It may be unsafe for whistleblowers and journalists to raise the alarm domestically, and international media reporting may not always be accessible.

Another example from Cambodia where sustained public relations campaigns distorted efforts to exercise due diligence is Prince Holding Group (discussed earlier in this brief) and its founder, Chen Zhi, who has acted as an advisor to the current and former Cambodian prime ministers.⁹³ Chen Zhi and more than 140 businesses and individuals associated with his network were sanctioned by the

US and UK governments in October 2025.⁹⁴ However, prior to the sanctions, Prince Holding Group commissioned an international content strategy⁹⁵ for its various businesses, such as Canopy Sands.⁹⁶ It also heavily promoted its corporate activities, ensuring positive messaging is readily available in online searches.

Meanwhile, Voice of Democracy, an independent news outlet that had published articles raising major ethical concerns over Prince and Canopy Sands long before the sanctions designation, was shut down by Cambodia's government in February 2023.⁹⁷ The government also blocked Radio Free Asia (RFA) a few months later.⁹⁸ This means RFA's rigorous three-part investigation into Chen Zhi and the Prince Holding Group cannot be accessed in-country. The RFA investigation delved into allegations of money laundering, illegal gambling operations, open arrest warrants in China and links to at least one scam compound where victims said they had been tortured.⁹⁹ This important work was largely flying under the radar of potential in-country partners. This included figures in diplomatic, business and NGO circles who were, and may continue to be, courted by Prince and who – by appearing in promotional materials and social posts with company representatives – might find they have been unwittingly exploited for image laundering purposes regardless of whether they ultimately sign any agreements.

Warnings about exposure to Prince Holding Group, however, were still issued by private risk analysis organizations and heeded by receptive governments and police agencies. For example, in March 2025, Pacific Economics, a Hawaii-based think-tank, told the governments of Taiwan and Palau that accepting further investment from Prince Holding Group could threaten their security and sovereignty.¹⁰⁰

More broadly, this example shows how restricted information channels affect the ability of partners, suppliers, developers and funding bodies to run background checks in other jurisdictions. In a move broadly celebrated by leaders in countries central to the cyber scam trade – including Cambodia, Myanmar and China¹⁰¹ – RFA announced that it expected to close after the administration of US President Donald Trump cut federal funding in March 2025.¹⁰²

Aside from Cambodia, access to RFA has been blocked in various jurisdictions where accurate information is vital for entities that need to conduct background checks on potential partners and projects, including Vietnam,¹⁰³ Myanmar¹⁰⁴ and mainland China.¹⁰⁵ Moreover, RFA closed its Hong Kong Bureau in 2024.¹⁰⁶ In Singapore, a leading source of foreign direct investment for countries vulnerable to scam compounds,¹⁰⁷ online articles can be censored if deemed to undermine 'public confidence in the integrity of the Singapore government'.¹⁰⁸ Singapore's two state-owned sovereign wealth funds, GIC¹⁰⁹ and Temasek,¹¹⁰ are investors in these countries. Two companies in Temasek's portfolio,¹¹¹ Surbana Jurong (SJ Group)¹¹² and Ascott (CaptiLand),¹¹³ were marketed heavily as key partners¹¹⁴ in Prince Group development projects in Cambodia,¹¹⁵ with the latter only terminating agreements following the US sanctions package in October 2025.¹¹⁶ Temasek has denied any responsibility, on the grounds that its companies provided 'professional services' and did not have an ownership stake.¹¹⁷

On the other hand, well-resourced figures with documented ties to the cyber scam industry increasingly pursue libel litigation against media outlets in countries where publications name them in reports.¹¹⁸ This was reflected, for example, in the removal of existing articles¹¹⁹ and a last-minute cancellation of stories on the cyber scam industry¹²⁰ due for publication by outlets in Australia in the wake of a string of lawsuits by a member of Cambodia's ruling Hun family.¹²¹



NOTES

- 1 GI-TOC, Compound crime: Cybercrime operations in Southeast Asia, May 2025, <https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/>.
- 2 Chainalysis, The 2025 crypto crime report, February 2025, <https://go.chainalysis.com/2025-Crypto-Crime-Report.html>.
- 3 Global Anti-Scam Alliance, International scammers steal over \$1 trillion in 12 months in global state of scams report 2024, 7 November 2024, <https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai>.
- 4 Statista, Global gross domestic product (GDP) at current prices from 1985 to 2029, October 2024, <https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp>.
- 5 Statista, Estimated cost of cybercrime worldwide 2018-2029, June 2024, <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>.
- 6 Lindsey Kennedy and Nathan Paul Southern, Cambodia's billion dollar scam, The Dial, 15 October 2024, <https://www.thedial.world/articles/news/issue-20/cambodia-cyber-scams-human-trafficking>.
- 7 Amanda Gore et al, Asian roulette: Criminogenic casinos and illicit trade in environmental commodities in South East Asia, GI-TOC, July 2022, <https://globalinitiative.net/analysis/casino-crime-south-east-asia/>.
- 8 GI-TOC, Compound crime: Cybercrime operations in Southeast Asia, May 2025, <https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-south-east-asia/>; Amanda Gore et al, Asian roulette: Criminogenic casinos and illicit trade in environmental commodities in South East Asia, GI-TOC, July 2022, <https://globalinitiative.net/analysis/casino-crime-south-east-asia/>.
- 9 GI-TOC, Global Organized Crime Index, Philippines, <https://ocindex.net/country/philippines>.
- 10 Al Jazeera, Cambodia's casino gamble: All in on Sihanoukville, 2019, <https://interactive.aljazeera.com/aje/2019/cambodia-casino-gamble/index.html>.
- 11 Presidential Communications Office, PBBM orders immediate ban against all PH POGO operations, Office of the President of the Philippines, November 2024, https://pco.gov.ph/news_releases/pbbm-orders-immediate-ban-against-all-ph-pogo-operations/.
- 12 Amanda Gore et al, Asian Roulette. Criminogenic casinos and illicit trade in environmental commodities in South East Asia, July 2022, GI-TOC, <https://globalinitiative.net/analysis/casino-crime-south-east-asia/>.
- 13 Lindsey Kennedy and Nathan Paul Southern, Cambodia's billion dollar scam, The Dial, 15 October 2024, <https://www.thedial.world/articles/news/issue-20/cambodia-cyber-scams-human-trafficking>.
- 14 Amanda Gore et al, Asian roulette: Criminogenic casinos and illicit trade in environmental commodities in South East Asia, GI-TOC, July 2022, <https://globalinitiative.net/analysis/casino-crime-south-east-asia/>.
- 15 Lindsey Kennedy and Nathan Paul Southern, Inside Southeast Asia's casino scam archipelago, The Diplomat, 2 August 2022, <https://thediplomat.com/2022/08/inside-southeast-asias-casino-scam-archipelago/>.
- 16 GI-TOC, Compound crime: Cybercrime operations in Southeast Asia, May 2025, <https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/>.
- 17 It is worth noting that She Zhijiang was arrested in Thailand on an INTERPOL red notice in 2022 and had been detained there since. In November 2025, he was extradited to China. He and his company Yatai have also been sanctioned by the US and UK for links to rights abuses in cyber scam compounds in their development. See Koh Ewe and Jonathan Head, Thailand extradites owner of Myanmar scam city to China, 12 November 2025, BBC, <https://www.bbc.co.uk/news/articles/cx20xx2pl69o>.
- 18 GI-TOC, Compound crime: Cybercrime operations in Southeast Asia, May 2025, <https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/>.
- 19 The Irrawaddy, Yatai IHG may seek to co-opt Myanmar government officials through dubious connections, 6 October 2020, <https://www.irrawaddy.com/news/burma/yatai-ihg-may-seek-to-co-opt-myanmar-government-officials-through-dubious-connections.html>.

- 20 Lulu Luo and Jonathan Head, The shadowy Chinese firms that own chunks of Cambodia, BBC News, 25 September 2023, <https://www.bbc.co.uk/news/world-asia-66851049>; Bora Ly, AVI Policy Brief: Belt and Road Initiative and tourism infrastructure investment in Cambodia, Asian Vision Institute, 17 February 2020, <https://asianvision.org/archives/publications/avi-policy-brief-issue-2020-no-02>.
- 21 Brenda Go and Prak Chan Thul, In Cambodia, stalled Chinese casino resort embodies Silk Road secrecy, risks, Reuters, 6 June 2018, <https://www.reuters.com/article/us-china-silkroad-cambodia-insight-idUSKCN1J20HA/>.
- 22 See, for example, the Dong Lecheng case study in Appendix 2 of this report.
- 23 It is important to note that despite their similar names, the authors have been unable to establish whether there is a deeper connection between KK Concrete and KK Park, and KK Concrete did not respond to requests for comment. Julia Bayer, Juliett Pineda and Yuchen Li, How Chinese mafia are running a scam factory in Myanmar, DW, 30 January 2024, <https://www.dw.com/en/how-chinese-mafia-are-running-a-scam-factory-in-myanmar/a-68113480>.
- 24 Photos and coordinates compiled between November 2024 and March 2025 by Cezary Podkul in Mae Sot, Thailand, which the GI-TOC research team has seen.
- 25 Erin West, Do you like good news?, LinkedIn, https://www.linkedin.com/posts/erinordbywest_whatifwecould-activity-7307731400072351745-bwSE/.
- 26 Cezary Podkul, Frontline updates from the Thai-Myanmar border, The Big Trace, March 2025, <https://buttondown.com/Cezary/archive/frontline-updates-from-the-thai-myanmar-border/>.
- 27 Information provided by Cezary Podkul, Mae Sot, July 2025.
- 28 DPD Data Warehouse (Thai government business registry), KK Concrete 2024, <https://datawarehouse.dbd.go.th/company/profile/ZGZvbums-JJQtPLDdiSMNlyoLFQZwGi8U7uKtiWtpgLml5rHXa-kufw2T87svvP>.
- 29 KK Concrete, Facebook profile, <https://www.facebook.com/profile.php?id=61558137096603>. Despite their similar names, we have been unable to establish whether there is a deeper connection between KK Park and either KK Concrete and Steel Limited Partnership (headquartered in Sisaket, with identical branding to the production facility photographed) and/or KK Concrete 2024 Co. Ltd (advertised on Facebook as based in Mae Sot as of July 2025). Neither KK Concrete nor KK Concrete 2024 responded to written requests for comment.
- 30 US Department of the Treasury, Treasury sanctions Zhao Wei transnational criminal organization, 30 January 2018, <https://home.treasury.gov/news/press-releases/sm0272>.
- 31 International Court of Justice, Submission of the International Commission of Jurists to the Committee on Economic, Social and Cultural Rights in advance of the examination of the International Covenant on Economic, Social and Cultural Rights, January 2023, https://www.icj.org/wp-content/uploads/2023/01/Final_ICJ_CESCR-CAMBODIA-SUB-2022.pdf.
- 32 U.S. Department of the Treasury, Treasury sanctions Southeast Asian networks targeting Americans with cyber scams, 8 September 2025, <https://home.treasury.gov/news/press-releases/sb0237>; U.S. Department of the Treasury, Treasury Sanctions Chinese Entity in Cambodia Under Global Magnitsky Authority, <https://home.treasury.gov/news/press-releases/sm1121>; U.S. Department of the Treasury, Treasury sanctions corruption and material support networks, 9 December 2019, <https://home.treasury.gov/news/press-releases/sm849>; HM Treasury, Office of Financial Sanctions Implementation, Financial Sanctions Notice, 8 December 2023, https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf; U.S. Department of the Treasury, Treasury sanctions the Zhao Wei Transnational Criminal Organization, 30 January 2018, <https://home.treasury.gov/news/press-releases/sm0272>.
- 33 Such methods can include employers confiscating passports or issuing incorrect visas, misrepresenting jobs, recruitment through networks of formal or informal brokers and debt bondage. These abuses are often exacerbated by a lack of support networks or complaint mechanisms once in-country, limited understanding of the local context, few connections and language barriers. Interview with Sharlene Chen, Head of Programmes at Humanity Research Consultancy, February 2025.
- 34 Naw Betty Han, Shwe Kokko: a paradise for Chinese investment, Frontier Myanmar, 5 September 2019, <https://www.frontiermyanmar.net/en/shwe-kokko-a-paradise-for-chinese-investment/>.
- 35 Ivan Franceschini, Building the new Macau: A portrait of Chinese construction workers in Sihanoukville, Made in China Journal, 25 January 2021, <https://madeinchinajournal.com/2021/01/25/building-the-new-macau-a-portrait-of-chinese-construction-workers-in-sihanoukville/>.
- 36 Joe Buckley and Christian Eckerlein, Cambodian labour in Chinese-owned enterprises in Sihanoukville: A study into the living and working conditions of Cambodian labourers in the construction, casino and manufacturing sectors, *Sozialpolitik*, 2, 2020, <https://doi.org/10.18753/2297-8224-163>.
- 37 Hul Reaksmey, A year on, workers still haunted by Sihanoukville building collapse, VOA, 28 June 2020, <https://khmer.voanews.com/a/a-year-on-workers-still-haunted-by-sihanoukville-building-collapse/5473659.html>.
- 38 Information provided by a Cambodian police officer involved in settlement negotiations between the family of an injured construction worker and the developer, May 2025.
- 39 Center for Alliance of Labour and Human Rights, Death toll in Cambodia building collapse rises to 28, 25 June 2019, <https://central-cambodia.org/archives/2841>.
- 40 Information provided by a Cambodian police officer involved in settlement negotiations between the family of an injured construction worker and the developer, May 2025.
- 41 Buth Reaksmey Kongkea, Justice served: Conviction in S'ville deadly building collapse case upheld, *Khmer Times*,

- 16 June 2022, <https://www.khmertimeskh.com/50109-4999/justice-served-conviction-in-sville-deadly-building-collapse-case-upheld/>.
- 42 World Bank, Listing of ineligible firms and individuals, February 2025, <https://www.worldbank.org/en/projects-operations/procurement/debarred-firms>.
- 43 AFP/Press Trust of India, Bangladesh blacklists Chinese firm over alleged bribe, *The New Indian Express*, 18 January 2018, <https://www.newindianexpress.com/pti-news/2018/Jan/18/bangladesh-blacklists-chinese-firmover-alleged-bribe-1757060.html>.
- 44 Sangam Prasain, ADB blacklists top Chinese construction firms, *The Kathmandu Post*, 20 December 2021, <https://kathmandupost.com/money/2021/12/20/adb-blacklists-top-chinese-construction-firms>.
- 45 Danielle Keeton-Olsen and Mech Dara, Prince-linked firm pours sand into 400 hectares of bay without study, VOD, February 2021, <https://vodenglish.news/prince-linked-firm-pours-sand-into-400-hectares-of-bay-without-study/>.
- 46 Construction & Property, Masterplan for \$16 billion Ream City development approved, 9 February 2021, <https://construction-property.com/masterplan-for-us16-billion-ream-city-development-approved/>.
- 47 Sreynat Sarum and Danielle Keeton-Olsen, Cambodia's Ream National Park transformed from wildlife park to development zone, *China Dialogue*, 5 April 2023, <https://chinadialogue.net/en/nature/cambodias-ream-national-park-transformed-from-wildlife-haven-to-development-zone/>.
- 48 Ibid.
- 49 Organized Crime and Corruption Reporting Project (OCCRP), South Korea sanctions sprawling "Prince Group", alleged criminal empire, November 2025, <https://www.occrp.org/en/news/south-korea-sanctions-sprawling-prince-group-alleged-criminal-empire>.
- 50 Office of Public Affairs, Chairman of Prince Group indicted for operating Cambodian forced labour scam compounds engaged in cryptocurrency fraud schemes, US Department of Justice, October 2025, <https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged>.
- 51 US Institute of Peace Senior Study Group, Transnational crime in Southeast Asia, May 2024, https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-south-east-asia.pdf; Jacob Sims, Policies and patterns, state-abetted transnational crime in Cambodia as a global security threat, May 2025, https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/68264cff356caba11f2db1e_Policies%20and%20Patterns_16052025.pdf.
- 52 Nicholas Farelly, Alice Dawkins and Patrick Deegan, Sihanoukville: A hub of environmental crime convergence, GI-TOC, September 2022, <https://globalinitiative.net/analysis/sihanoukville-hub/>; Amnesty International, "I was someone else's property": slavery, human trafficking and torture in Cambodia's scamming compounds, June 2025, <https://www.amnesty.org/en/wp-content/uploads/2025/06/ASA2394472025ENGLISH.pdf>.
- 53 Jack Adamović Davies, Cambodia's Prince Group: An empire built on crime?, RFA, 5 February 2024, <https://www.rfa.org/english/special-reports/prince-group/>.
- 54 See Wangcang County People's Court, Sichuan Province, 利用境外软件赌博捞钱，魔高一尺 依法审判构建网络安全，道高一丈, 13 July 2022, accessed via Archive Today, <https://archive.ph/2023.06.13-075727/http://gywcfy.scssfw.gov.cn/article/detail/2022/07/id/6792102.shtml>.
- 55 ADB, Yunnan Lincang border economic cooperation zone development project, Regional cooperation and integration summary, <https://www.adb.org/sites/default/files/linked-documents/49310-002-sd-01.pdf>.
- 56 OECD, Responsible business conduct and anti-corruption compliance in Southeast Asia: Practices, progress and challenges, 2021, <https://www.undp.org/asia-pacific/fairbiz/publications/responsible-business-conduct-and-anti-corruption-compliance-southeast-asia>.
- 57 Ibid.
- 58 Ibid.
- 59 Ibid.
- 60 Interview with Sharlene Chen, Head of Programmes at Humanity Research Consultancy, February 2025.
- 61 Ibid.
- 62 Roxanne Wang, A key figure behind She Zhejiang, the detained tycoon of cyber scam hubs, 163.com, 25 February 2025, <https://www.163.com/money/article/JP8KO79A00259RLO.html>.
- 63 She Zhejiang was arrested in Thailand in 2022 on an international warrant and an INTERPOL red notice for allegedly running illegal online gambling operations. The US has linked She to scam and trafficking networks. He will be extradited to China to stand trial. See Alleged gambling kingpin linked to scam centres extradited from Thailand to China, *The Guardian*, 13 November 2025, <https://www.theguardian.com/world/2025/nov/13/alleged-gambling-kingpin-she-zhejiang-extradited-thailand-china>; Cyber Scam Monitor, She Zhejiang criminal judgement, March 2015, <https://web.archive.org/web/20230323132735/https://cyberscammonitor.net/wp-content/uploads/2022/10/She-Zhejiang-Criminal-Judgement.pdf>.
- 64 *The Bangkok Post*, She Zhijiang remains dedicated to charity amidst challenging times, 19 July 2023, <https://www.nationthailand.com/pr-news/more/pr-news/40029503>; The Irrawaddy, Contracts reveal KNU involvement in notorious Myanmar scam center, 3 April 2024, <https://www.irrawaddy.com/news/investigation/contracts-reveal-knu-involvement-in-notorious-myanmar-scam-center.html>.
- 65 Office of Financial Sanctions Implementation, HM Treasury, Human rights sanctions announcement, 8 December 2023, https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf.

- 66 Jared Ferrie et al, Gambling tycoon's partners abandon him as extradition to China looms, OCCRP, 26 July 2023, <https://www.occrp.org/en/daily/17874-gambling-tycoon-s-partners-abandon-him-as-extradition-to-china-looks>.
- 67 The World Bank, Notice of uncontested sanctions proceedings, March 2020, [https://www.worldbank.org/content/dam/documents/sanctions/office-of-suspension-and-debarment/2020/mar/Case%20641%20-%20Notice%20of%20Uncontested%20Sanctions%20Proceeding%20\(3.23.2020\).pdf](https://www.worldbank.org/content/dam/documents/sanctions/office-of-suspension-and-debarment/2020/mar/Case%20641%20-%20Notice%20of%20Uncontested%20Sanctions%20Proceeding%20(3.23.2020).pdf).
- 68 Ibid.
- 69 UK Government, UK and allies sanction human rights abusers, 8 December 2023, <https://www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers>.
- 70 US Department of the Treasury, Treasury sanctions Southeast Asian networks targeting Americans with cyber scams, 8 September 2025, <https://home.treasury.gov/news/press-releases/sb0237>.
- 71 Ibid.
- 72 Mary Ann Jolley, Cambodia's cyber slaves, ABC News, 15 March 2023, <https://www.abc.net.au/news/2023-03-15/cambodias-cyber-slaves/102096904>.
- 73 *Khmer Times*, Yunnan Jingcheng Group Co., Ltd strongly deny charges of 'human trafficking, fraud, cyber fraud', 23 August 2022, <https://www.khmertimeskh.com/501137150/yunnan-jingcheng-group-co-ltd-strongly-deny-charges-of-human-trafficking-fraud-cyber-fraud/>.
- 74 Mary Ann Jolley, Cambodia's cyber slaves, ABC News, 15 March 2023, <https://www.abc.net.au/news/2023-03-15/cambodias-cyber-slaves/102096904>.
- 75 Yunnan Jingcheng Group Co. Ltd, Jincheng Group purchased a land purchase agreement for sea view houses in Cambodia, 2018, <http://www.jcjtgs.com/content-9-1222-1.html>.
- 76 Mary Ann Jolley, Cambodia's cyber slaves, ABC News, 15 March 2023, <https://www.abc.net.au/news/2023-03-15/cambodias-cyber-slaves/102096904>.
- 77 Kris Janssens, *Sihanoukville, gokparadijs en Chinese enclave in Cambodja*, Mondiaal Nieuws, 13 August 2018, <https://www.mo.be/reportage/sihanoukville-gokparadijs-en-chinese-enclave-cambodja>.
- 78 Robin Spiess, How Cambodia can make the most of China's millions, *Southeast Asia Globe*, 22 May 2019, <https://southeastasiaglobe.com/how-cambodia-can-make-the-most-of-chinas-millions/>.
- 79 Cyber Scam Monitor, Kaibo, 22 February 2022, <https://web.archive.org/web/20221114005526/https://cyberscammonitor.net/profile/kaibo/>.
- 80 Mao Pengfei and Nguon Sovan, Interview: China-aided rural projects playing vital role in improving Cambodia's economy, people's livelihoods: Cambodian official, *Xinhua*, 22 February 2021, https://web.archive.org/web/20221126035633/http://www.xinhuanet.com/english/2021-02/22/c_139759036.htm.
- 81 Graeme Smith, Public goods, piety and place: The legitimization strategies of local business elites in China, in *Local Elites in Post-Mao China*, edited by Yingjie Guo, Routledge, 2018.
- 82 Ibid.
- 83 Ibid.
- 84 Ibid.
- 85 UK Office of Financial Sanctions, Financial sanctions notice: Global human rights, HM Treasury, December 2023, https://assets.publishing.service.gov.uk/media/6572d54804951600d49be78/Notice_Global_Human_Rights_081223.pdf; US Department of the Treasury, Treasury sanctions Southeast Asian networks targeting Americans with cyber scams, 8 September 2025, <https://home.treasury.gov/news/press-releases/sb0237>.
- 86 Cyber Scam Monitor, X (formerly Twitter) post, 8 February 2024, <https://x.com/CyberScamWatch/status/1755615827716641177>.
- 87 US Department of the Treasury, Treasury sanctions criminal network of Zhao Wei, 30 January 2018, <https://home.treasury.gov/news/press-releases/sm0272>.
- 88 UK Government, Press release: UK and allies sanction human rights abusers, 8 December 2023, <https://www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers>.
- 89 Cyber Scam Monitor, X (formerly Twitter) post, 8 February 2024, <https://x.com/CyberScamWatch/status/1755615827716641177>.
- 90 Sebastian Strangio, Laos bestows national development award on sanctioned Chinese 'crime boss', *The Diplomat*, December 2024, <https://thediplomat.com/2024/12/laos-bestows-national-development-award-on-sanctioned-chinese-crime-boss/>.
- 91 *Nordic Chinese Times*, 双语:老挝政府授予金三角经济特区管委会主席赵伟先生“国家三级发展贡献勋章”, *China News*, 6 December 2024, <http://www.chinanews.se/static/content/BOSQ/2024-12-05/1315397024917250048.html>.
- 92 Reporters Without Borders, World Press Freedom Index, 2025, <https://rsf.org/en/index>.
- 93 Jonathan Head, The mysterious figure accused of masterminding a \$14bn crypto scam, *BBC News*, 24 October 2025, <https://www.bbc.co.uk/news/articles/c70jz8e00g1o>.
- 94 Office of Foreign Assets Control, Transnational Criminal Organizations Designations; Issuance of TCO-related General License, 14 October 2025, <https://ofac.treasury.gov/recent-actions/20251014>; UK Government, UK Sanctions List Designation, 14 October 2025, <https://search-uk-sanctions-list.service.gov.uk/designations/GHR0179/Individual>.
- 95 Paid-for advertorials and company steered articles/interviews that can be hard to distinguish from genuine news coverage.
- 96 An example of such sponsored content can be found here: Canopy Sands, Ream city: The plan to transform Sihanoukville into a green living hub, *Eco-Business*, 12 November 2021, <https://www.eco-business.com/news/ream-city-the-plan-to-transform-sihanoukville-into-a-green-living-hub/>.

- 97 Amnesty International, Cambodia: Shuttering 'Voice of Democracy' is attempt to slam door on independent media, 13 February 2023, <https://www.amnesty.org/en/latest/news/2023/02/cambodia-shuts-down-voice-democracy-media/>.
- 98 Noeurn Davin and Lora LibLib, Cambodian government blocks news sites before unopposed election, VOA, 17 July 2023, <https://www.voanews.com/a/cambodian-government-blocks-news-sites-before-unopposed-election-/7185151.html>.
- 99 Jack Adamovic Davies and Mary Zhao, Chinese courts go after 'notorious' Cambodian conglomerate, RFA, 5 February 2024, <https://www.rfa.org/english/news/cambodia/prince-group-investigation-02022024124011.html>.
- 100 Jack Adamović Davies and Jane Tang, Pacific governments warned of 'threat' from Cambodia's Prince Group, RFA, March 2025, <https://www.rfa.org/english/cambodia/2025/03/12/corruption-security-taiwan-palau>.
- 101 Sebastian Strangio, Cambodia's Hun Sen, Myanmar junta celebrate closure of US-funded media outlets, *The Diplomat*, 18 March 2025, <https://thediplomat.com/2025/03/cambodias-hun-sen-myanmar-junta-celebrate-closure-of-us-funded-media-outlets/>.
- 102 David Folkenflik, 'Bloody Saturday' at Voice of America and other US-funded networks, NPR, 15 March 2025, <https://www.npr.org/2025/03/15/nx-s1-5329244/bloody-saturday-voiceofamerica-radio-free-asia-europe-trump-kari-lake>.
- 103 Reporters Without Borders, Radio Free Asia, <https://rsf.org/en/radio-free-asia>.
- 104 Associated Press, Myanmar cracks down on flow of information by blocking VPNs, VOA News, 14 June 2024, <https://www.voanews.com/a/myanmar-cracks-down-on-flow-of-information-by-blocking-vpns-/7657052.html>.
- 105 Jim Mann, Republican voltage keeps Radio Free Asia buzzing, *Los Angeles Times*, 1 October 1997, <https://www.latimes.com/archives/la-xpm-1997-oct-01-mn-38101-story.html>.
- 106 *The Guardian*, US-funded Radio Free Asia shuts down in Hong Kong over safety concerns, 30 March 2024, <https://www.theguardian.com/world/2024/mar/30/us-funded-radio-free-asia-shuts-down-in-hong-kong-over-safety-concerns>.
- 107 Singapore Department of Statistics, Singapore's direct investment abroad by destination economy 2013-2023, <https://tablebuilder.singstat.gov.sg/table/TS/M084431>.
- 108 Freedom House, Singapore, Freedom on the Net 2020 country report, <https://freedomhouse.org/country/singapore/freedom-net/2020n>.
- 109 *The Business Times*, Singapore remains a significant investor in the Philippines, 10 June 2021, <https://www.businesstimes.com.sg/international/philippines-independence-day/singapore-remains-significant-investor-philippines>; Bloomberg UK, Singapore's GIC bets on Latin American infrastructure companies, 10 May 2024, <https://www.bloomberg.com/news/articles/2024-05-10/singapore-s-gic-bets-on-latin-american-infrastructure-companies>; Jonathan Brasse, GIC makes Africa play backing two biggest firms, PERE, 2 March 2016, <https://www.perenews.com/gic-makes-africa-play-backing-two-biggest-firms-exclusive/>.
- 110 *Khmer Times*, Temasek Holding Company in Singapore aims to expand its business in Cambodia, 18 January 2024, <https://www.khmertimeskh.com/501425185/temasek-holdings-company-in-singapore-aims-to-expand-its-business-in-cambodia/>; Claire Hammond, Temasek and ADB back Myanmar investment fund, *Frontier Myanmar*, 18 January 2019, <https://www.frontiermyanmar.net/en/temasek-and-adb-back-myanmar-investment-fund/>; Alex Dooler, Temasek's \$54 billion asset management unit opens Abu Dhabi office, *Bloomberg*, 24 March 2025, <https://www.bloomberg.com/news/articles/2025-03-24/temasek-s-54-billion-asset-management-unit-opens-abu-dhabi-office>.
- 111 Low De Wei and David Ramli, Singapore ties to multibillion scam case in spotlight, *Bloomberg*, 16 October 2025, <https://www.bloomberg.com/news/articles/2025-10-16/singapore-ties-to-alleged-cambodian-pig-butcherer-scam-ring-under-spotlight>.
- 112 Jack Board, In Focus: Cambodia's \$16billion 'eco-city' raises financial and economic concerns, *Channel News Asia*, 4 May 2024, <https://www.channelnewsasia.com/asia/cambodia-sihanoukville-bay-lights-eco-city-prince-group-4252091>.
- 113 Cambodia Investment Review, Bay of Lights partners Ascott, setting new standards for luxury and hospitality in Sihanoukville, Cambodia, 11 April 2024, <https://cambodiainvestmentreview.com/2024/04/11/bay-of-lights-partners-ascott-setting-new-standards-for-luxury-and-hospitality-in-sihanoukville-cambodia/>.
- 114 Gayle Goh, Surbana Jurong's masterplan for US \$16bn 'Ream City' in Sihanoukville gets go-ahead, *The Straits Times*, 8 February 2021, <https://www.straitstimes.com/business/companies-markets/surbana-jurongs-masterplan-for-16b-ream-city-in-cambodia-gets-green-light>.
- 115 Promotional videos have mostly been removed by all parties, but press releases replicated across other platforms and news sites highlight the partnerships. For example, this press release was published by sites in Cambodia, Macau, Dubai, Taiwan, Malaysia and various countries in September 2024, seen here in the *Khmer Times*: <https://www.khmertimeskh.com/501553846/bay-of-lights-a-visionary-transformation-of-cambodias-coastline-showcased-at-the-inaugural-singapore-business-expo/>.
- 116 Temasek, Statement on Bloomberg article: Misleading framing of Temasek's role, 17 October 2025, <https://www.temasek.com.sg/en/news-and-resources/news-room/statements/2025/statement-on-bloomberg-article-misleading-framing-of-temasek-role>.
- 117 Ibid.
- 118 Lindsey Kennedy and Nathan Paul Southern, The sanction effect: Designating cyber scam networks helps protect those exposing them against legal challenges, GI-TOC,

28 October 2025, <https://globalinitiative.net/analysis/designating-cyber-scam-networks-helps-protect-those-exposing-them-against-legal-challenges/>.

- 119 UCA News, Australian daily clarifies story that offended Hun Sen's nephew, 16 July 2024, <https://www.ucanews.com/news/australian-daily-clarifies-story-that-offended-hun-sens-nephew/105726>.

120 Based on confidential conversations with freelance journalists and internal research, 2024 and 2025.

- 121 Lawyerly, Serious harm question won't be heard first in defamation case over 'cyberslaves' doco, 19 September 2023, <https://www.lawyerly.com.au/court-rejects-separate-hearing-on-serious-harm-in-defamation-case-over-cambodian-cyberslaves-doco/>.



**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

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

www.globalinitiative.net