United Nations
Office on Drugs and Crime

Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia

April 2025



Technical Policy Brief

Copyright © 2025, United Nations Office on Drugs and Crime (UNODC).

This publication may not be reproduced in whole or in part and in any form for educational or non-profit purposes without special permission from the copyright holder, provided acknowledgement of the source is made. UNODC would appreciate receiving a copy of any publication that uses this publication as a source.

Acknowledgements

Preparation of this report would not have been possible without data, information and intelligence shared by governments of East and Southeast Asia, international partners, and other organizations. This study was conducted by the UNODC Regional Office for Southeast Asia and the Pacific (ROSEAP) with the support of research experts of UNODC field offices based in Brazil, Latin America, Middle East and North America, South Africa, and West Africa, as well as several experts in the field.

Supervision
Benedikt Hofmann, Regional Representative a.i. (Supervision and technical review)

Core team
John Wojcik, Regional Analyst (Coordination, analysis and drafting)
Mark Bo, Senior Analyst (Analysis and drafting)
Seong Jae Shin, Regional Analyst (Analysis and drafting)
Dylan Hartnett, Regional Analyst (Analysis and drafting)
Inshik Sim, Lead Analyst (Technical review)
Fabrizio Fioroni, Regional Anti-Money Laundering Advisor (Technical review)
Aibek Turdukulov, Programme Officer (Technical review)
Rebecca Miller, Regional Programme Coordinator (Technical review)
Sylwia Gawronska, Regional Programme Advisor (Technical review)
Annika Wythes, Team Lead, Regional Anti-Corruption Hub (Technical review)
Joshua James, Regional Cybercrime Coordinator (Technical review)
Akara Umapornsakula (Graphic design)

This report has also benefited from the valuable input of many UNODC staff members and external experts and organizations who reviewed or contributed to various sections of the report including John Tobon, Thomas Dixon, Li Anne Lim, Jerry Davydov, Jisu Kim, Himal Ojha, Lorenzo Piacentini, Hieu Minh Ngo, Cezary Podkul, Jack Davies, Philippe Auclair, Renée Burton, Maël Le Touz, Nguyen Nguyen, Martin Young and Kelana Wisnu.

UNODC expresses its appreciation to organizations providing information, data and analytical support to this study including Beosin, Chainalysis, ChongLuaDao (Viet Nam), Crystal Blockchain, CyberArmor, Elliptic, Group-IB, Infoblox Threat Intel, Kroll, and TRM Labs.

Disclaimer

This report has not been formally edited.

The contents of this publication do not necessarily reflect the views or policies of UNODC, Member States, or contributory organizations, and neither do they imply any endorsement.

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of UNODC or the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Explanatory note

Reference to dollars ($) are to United States dollars, unless otherwise stated. Reference to tons are to metric tons, unless otherwise stated. Conversions and statistics presented in this report are current as of the time of printing.

UNITED NATIONS OFFICE ON DRUGS AND CRIME

Southeast Asia and the Pacific

Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia

April 2025

Technical Policy Brief

Table of Contents

Abbreviations and acronyms i

List of figures, tables and maps iii

Executive summary 1

Report development and analysis 15

Regional overview 19

Select case studies 63

Conclusion and recommendations 77

Abbreviations and acronyms

AML	Anti-Money Laundering
BGF	Border Guard Force
BPO	Business Processing Outsourcing Operations
CDN	Content Delivery Networks
DKBA	Democratic Karen Buddhist Army
DNS	Domain Name System
ERN	Emergency Response Network
FDI	Foreign Direct Investment
GTSEZ	Golden Triangle Special Economic Zone
KNLA	Karen National Liberation Army
KNU	Karen National Union
KYC	Know Your Customer
MNDAA	Myanmar National Democratic Alliance Army
OFAC	Office of Foreign Assets Control
PAGCOR	Philippine Amusement and Gaming Corporation
PoC	Province of China
POGO	Philippine Offshore Gaming Operator
P2P	Peer to peer
RAG	Retrieval Augmented Generation
RMB	Renminbi
SAC	State Administration Council
SAR	Special Administrative Region
SEC	Securities and Exchange Commission (Philippines)
SEZ	Special Economic Zone
SR	Special Region
STRs	Suspicious Transaction Reports
TOC	Transnational Organized Crime
UNODC	United Nations Office on Drugs and Crime
USDT	Tether Stable Coin
UWSA	United Wa State Army
VASPs	Virtual Asset Service Providers

List of figures, tables and maps

Executive summary

Map 1. Locations of known or reported scam centres in the Mekong region 2023 – 2025
Map 2. Origins of people identified in regional scam compounds
Figure 1. Expansion of select sites hosting cyber-enabled fraud operations, 2022 - 2025
Figure 2. Value of cryptocurrency inflows received by wallets used by Huione Guarantee and its vendors, 2021 – 2024

Regional overview

Map 1. Locations of known or reported scam centres in the Mekong region 2023 – 2025
Map 2. Origins of people identified in regional scam compounds
Table 1. Breakdown of workers removed from Myawaddy compounds in February, 2025
Figure 1. Expansion of select sites hosting online gambling and cyber-enabled fraud operations 2021 – 2025
Figure 2. Simplified illegal online gambling supply chain
Figure 3. Utility of illegal betting for large-scale money laundering and underground banking
Figure 4. Value of cryptocurrency inflows received by wallets used by Huione Guarantee and its vendors, 2021 – 2024
Figure 5. Value of estimated cryptocurrency inflows of largest illicit online marketplaces of all time
Figure 6. Simplified mirror transaction model used by the Xizhi Li network

Select case studies

Figure 1. Simplified network chart involving select suspects implicated in the Singapore money laundering case and elsewhere



Executive summary



Executive summary

Transnational organized crime in Southeast Asia is evolving faster than at any previous point in history. This was first observed in the shift to synthetic drug production, and particularly methamphetamine in Shan State, Myanmar, with supply surging to record levels year on year over the past decade. Less visible, however, was a more complex and far-reaching parallel shift that has fundamentally reshaped the regional threat landscape and criminal ecosystem.

This transformation has been marked by the proliferation of industrial scale cyber-enabled fraud and scam centres, driven by sophisticated transnational syndicates and interconnected networks of money launderers, human traffickers, data brokers, and a growing number of other specialist service providers and facilitators. It follows years of mounting enforcement and regulatory efforts targeting cross-border cash movement and money laundering related to unregulated casinos and online gambling operations commonly used as fronts for criminal activities – with many physically relocating and converging around inaccessible and autonomous non-state armed group-controlled territories, Special Economic Zones (SEZs), and other vulnerable border areas across the region, especially in the Mekong, which have served as breeding grounds for criminal networks.

As a result, Asian crime syndicates have emerged as definitive market leaders in cyber-enabled fraud, money laundering, and underground banking globally, actively enhancing collaboration with other major criminal networks around the world. These groups have grown rapidly in recent years, demonstrating their ability to adapt to and capitalize on changes in political and business environments, exploit gaps in governance and regulations, and rapidly develop advanced physical and digital infrastructure while integrating new business models and technologies including malware and artificial intelligence into their operations.

The situation has been further compounded by the rise of new illicit online marketplaces native to Southeast Asia which have dramatically expanded criminal revenue streams and enabled transnational organized crime to scale up operations. The emergence of these platforms has not only created new opportunities to expand physical bases of operation overseas, but is increasingly being used by criminal groups outside of Southeast Asia to launder proceeds of crime and circumvent formal financial systems. In response to new opportunities presented by the ability of illicit actors to connect in new ways and expand cooperation globally, service providers utilizing these platforms have shown growing signs of specialization within certain high-demand jurisdictions and financial institutions around the world.

As a growing number of governments intensify their efforts against cyber-enabled fraud and scam centres in the region, organized crime has responded by hedging both within and beyond it. It is now increasingly clear that a potentially irreversible spillover has taken place in Southeast Asia, leaving criminal groups free to pick, choose, and move jurisdictions, operations, and value as needed,

with the resulting situation rapidly outpacing the capacity of governments to contain it. More than this, the region has emerged as a key testing ground for organized crime, which is reflected in increasing linkages to criminal ecosystems in other parts of the world facing similar vulnerabilities and challenges.

Expanding on UNODC's past analyses of casinos, underground banking, technological innovation, and transnational organized crime in Southeast Asia, the development of this report has required analysis of law enforcement investigations, prosecutions, and related open-source information and monitoring, which has provided near real-time insights into the region's shifting threat landscape. More specifically, it has been developed through examination of criminal indictments, case records, court filings, intelligence analysis, and corporate data, as well as consultation with both international and regional law enforcement and criminal intelligence partners. UNODC has also conducted an extensive mapping and analysis of data obtained from thousands of illicit online marketplaces, groups, and channels attributed to regional criminal networks and affiliated service providers.

This report presents information, trends, and data points that have not previously been pieced together, representing a unique attempt to improve situational awareness about the intensifying global impacts and implications of the present situation, recognizing that the international community now stands at a critical inflection point. Failure to address this self-sustaining ecosystem will have unprecedented consequences for Southeast Asia that reverberate globally, as Asian crime syndicates continue to reinvest, professionalize, and integrate advanced technologies and capabilities allowing them to evolve into becoming more sophisticated cyber threat actors.

The study provides recommendations to improve knowledge, awareness, policy, capacity, and coordination, and aims to serve as a foundation for accelerated solutions and deeper engagement between countries in Southeast Asia and their international partners.

Operational adaptation, expansion, and evolution

Driven by billions in illicit capital inflows, cyber-enabled fraud and scam centres have taken on industrial proportions in Southeast Asia, with independent and scattered fraud gangs being replaced by larger, consolidated criminal groups often operating under the guise of industrial and science and technology parks as well as casinos and hotels.

Amidst heightened awareness and enforcement action taken by governments to address the crisis, Asian crime syndicates have sought to hedge their risk and ensure business continuity by expanding new and existing operations deeper into many of the most remote, vulnerable, and underprepared parts of Southeast Asia, and increasingly other regions. The dispersal of these sophisticated criminal networks within areas of weakest governance has attracted new players, fueled corruption, and enabled the industry to continue to scale, culminating in hundreds of large-scale scam operations conservatively generating tens of billions of dollars in annual profits.[1] In the United States alone, authorities reported more than US $5.6 billion in financial losses to cryptocurrency scams in 2023, with an estimated US $4.4 billion attributed to so-called 'pig butchering' schemes most prevalent in Southeast Asia.[2] Regionally, countries in East and Southeast Asia combined have lost up to an estimated US $37 billion to cyber-enabled fraud during that same year according to latest available data, with much larger estimated losses being reported globally.[3]

Like any multinational company, transnational criminal enterprises seek out conducive conditions that protect and insulate their businesses and ensure limited government interference. In so doing, major crime groups have converged around and, in many cases, infiltrated venues and businesses including casinos, SEZs, business parks, and various traditional financial and virtual asset services that have proven to offer all of the conditions, infrastructure, and regulatory, legal,

1 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*.

2 Federal Bureau of Investigation, "2023 Internet Crime Report", available at: https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf.

3 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*.

Figure 1. Expansion of select sites hosting cyber-enabled fraud operations, 2022 - 2025



KK Park, Myawaddy, Myanmar, April 2022 to December 2024. Source: Google Earth.



Pursat, Cambodia, February 2022 to January 2025. Source: Google Earth.



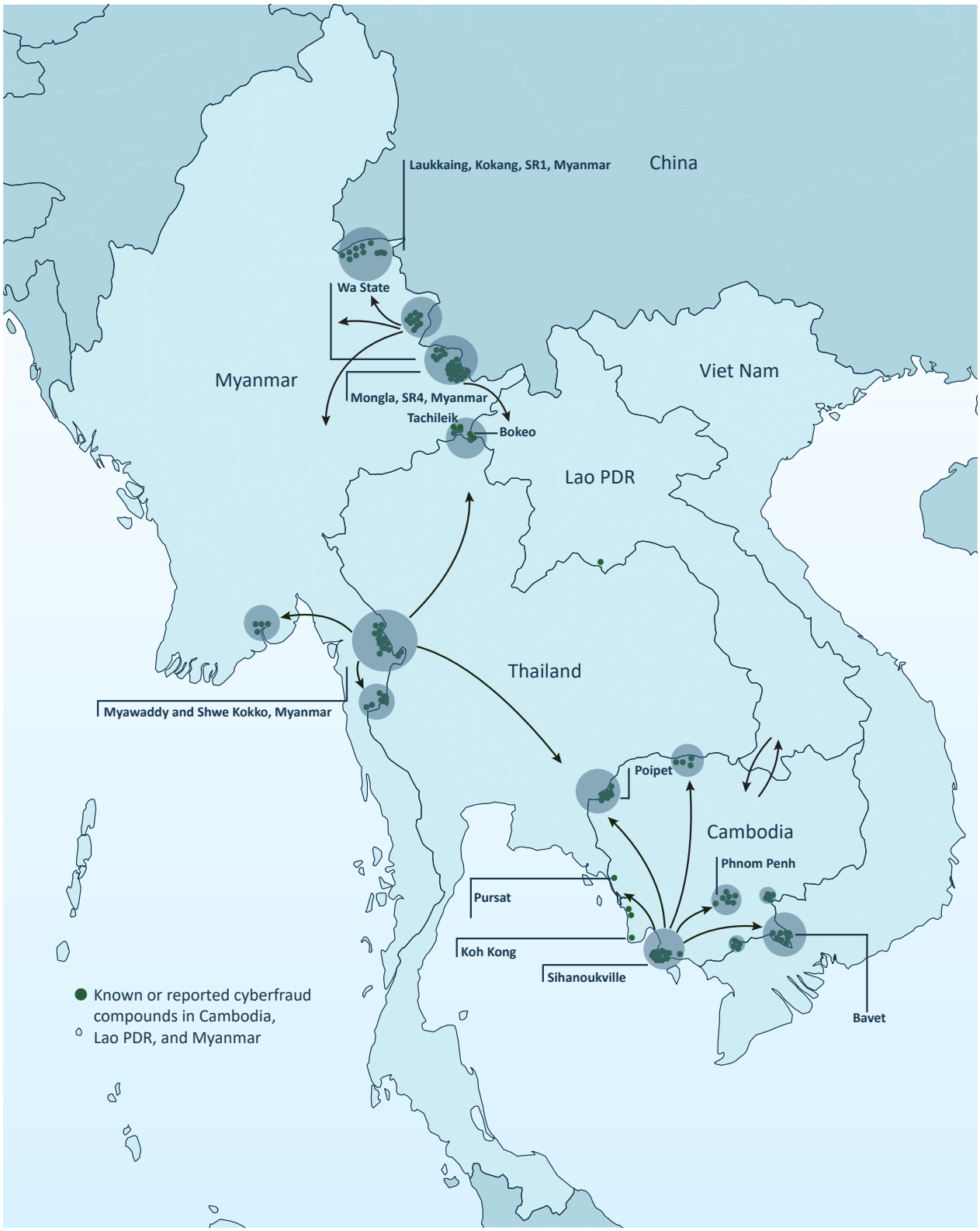
Tbong Khmum, Cambodia, December 2023 to January 2025. Source: Google Earth.

and fiscal covers required for sustained growth and expansion. This approach has proven highly effective, giving rise to a sprawling, interconnected ecosystem within which organized crime syndicates exploit gaps and vulnerabilities, jeopardize state sovereignty, and distort and corrupt policy-making processes and other government systems.

Against this backdrop, many of the region's largest criminal groups that have expanded within Southeast Asia and a growing number of jurisdictions in other parts of the world have rapidly diversified their business lines towards the development of key infrastructure. This has extended far beyond the construction and management of physical scam centres to include online gambling platforms and software services, unlicensed payment processors and cryptocurrency exchanges, encrypted communications platforms and, most recently, stablecoins,[4] blockchain networks, and illicit online marketplaces, often controlled by the same criminal networks. These groups have also developed robust multi-lingual workforces comprised of hundreds of thousands of trafficked victims and complicit individuals. Taken together, these developments have rapidly enabled Asian crime syndicates to broaden the scope of fraud victims being targeted globally, exacerbating existing challenges faced by law enforcement.

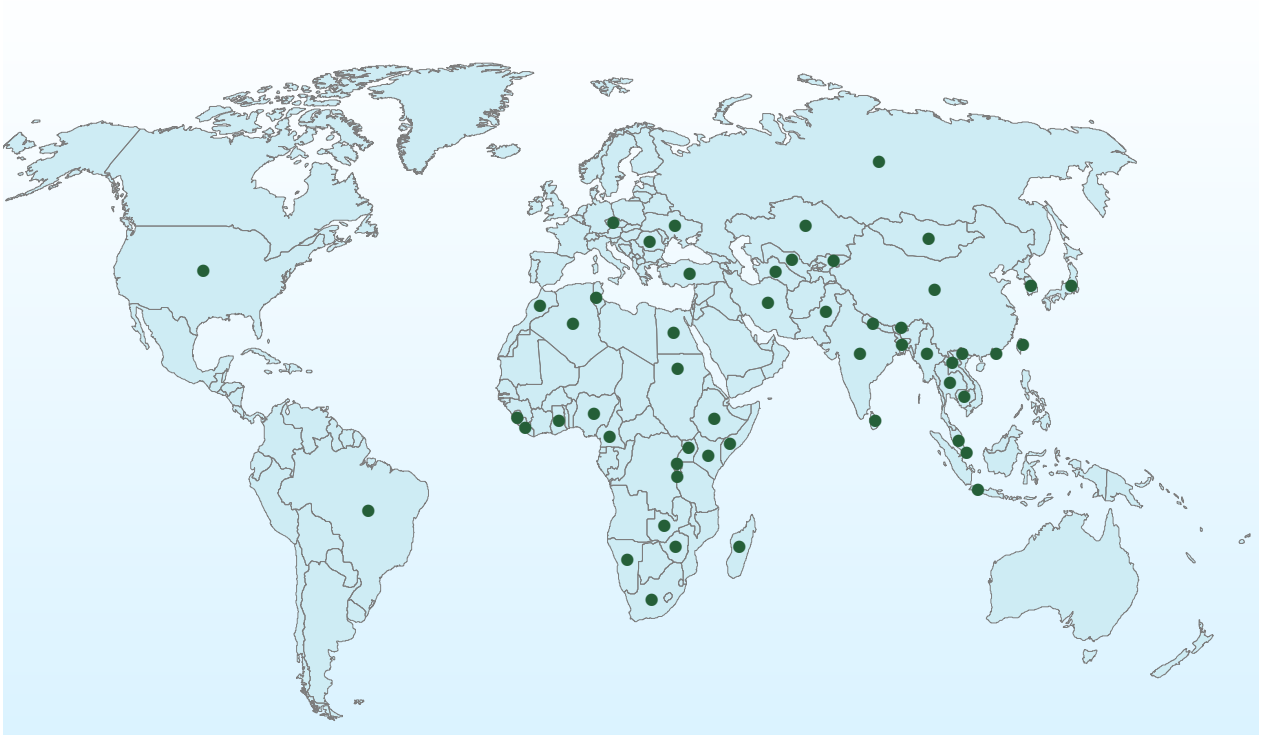
4 Stablecoins are cryptocurrencies pegged to and backed by fiat currencies such as the U.S. Dollar.

Map 1. Locations of known or reported scam centres in the Mekong region 2023 - 2025



Online operations and workers move both within and across borders in the Mekong region. Source: UNODC.

Map 2. Origins of people identified in regional scam compounds



Africa	**East Asia**	**Central Asia**
1. Algeria	23. China	43. Kazakhstan
2. Burundi	24. Hong Kong SAR	44. Kyrgyzstan
3. Cameroon	25. Japan	45. Turkmenistan
4. Egypt	26. Mongolia	46. Uzbekistan
5. Ethiopia	27. Republic of Korea	**West Asia**
6. Ghana	28. Taiwan PoC	47. Iran
7. Kenya	**Southeast Asia**	**Asia/Europe**
8. Liberia	29. Cambodia	48. Georgia
9. Madagascar	30. Indonesia	49. Russia
10. Morocco	31. Lao PDR	50. Türkiye
11. Mozambique	32. Malaysia	**Europe / North America**
12. Namibia	33. Myanmar	51. Czechia
13. Nigeria	34. Singapore	52. Romania
14. Rwanda	35. Thailand	53. Ukraine
15. Sierra Leone	36. Viet Nam	54. United States
16. Somalia	**South Asia**	**South America**
17. South Africa	37. Bangladesh	55. Brazil
18. Sudan	38. Bhutan	56. Colombia
19. Tunisia	39. India	
20. Uganda	40. Nepal	
21. Zambia	41. Pakistan	
22. Zimbabwe	42. Sri Lanka	

Source: UNODC review of official reports, statement from embassies and foreign affairs ministries, information provided by anti-trafficking in persons organizations. Note: There are likely to be more nationalities and places of origin that authorities are not yet aware of.

Criminal groups and service providers based in the region have also been quick to respond to mounting law enforcement pressure by capitalizing on the diffusion of powerful and increasingly accessible new technologies including blockchain, cloud computing, generative artificial intelligence, and machine learning, among others. This has provided them with a range of opportunities to develop new fraud capabilities and rely more heavily on technological processes to improve existing tactics and techniques, and expand channels for obfuscating and laundering criminal proceeds.

Geographic shifts and spillover beyond Southeast Asia

Globalized crime networks centred in Southeast Asia continue to demonstrate their ability to adapt to changes in political and business environments driven by increasing enforcement action targeting cyber-enabled fraud, money laundering, and underground banking. In response, these agile syndicates have expanded and partially hedged against shifting market dynamics in the region, seeking out other jurisdictions with similar characteristics, opportunities, and vulnerabilities to target and exploit.

Similarly to some of the most vulnerable parts of Southeast Asia, many countries beyond the region witnessing significant increases in illicit activity involving Asian crime syndicates face a variety of challenges in addressing the evolving situation. This ranges from limited human and technical resources (including forensic and investigative capacity), inter-agency coordination, international cooperation, and intelligence sharing to cope with the scale of the problem, as well as high rates of corruption which criminal actors can leverage.

Recent trends and incidents in countries outside of Southeast Asia are taking place where awareness and understanding of emerging threats, crime types, modus operandi, and technologies leveraged by Asian criminal groups is low, leaving many jurisdictions vulnerable and underprepared. More developed countries with more robust capacity to address transnational crime have also proven susceptible and exposed to the ability of Asian criminal networks to infiltrate these jurisdictions by targeting gaps in anti-money laundering and due diligence frameworks, and utilizing complex shell structures and vast, increasingly digital underground banking systems to obscure the origins of their wealth and shift value across borders undetected.

Over the past few years, this has culminated in several large overseas raids and crackdowns targeting scam centres with major ties to criminal networks in Southeast Asia, including those found operating in Africa, the Middle East, South Asia, and select Pacific islands, as well as related money laundering, trafficking in persons, and recruitment services as far as Europe, North America, and South America. The subtle and ongoing spillover creeping into other regions has allowed Asian crime syndicates to broaden the scope of their operations and target an increasingly diverse range of victim profiles and nationalities from around the world. More than this, it has allowed them to dramatically scale up profits and influence while simultaneously generating billions in illicit capital reserves (fiat and cryptocurrency) that can be reinvested into further expansion and also utilized to service the money laundering needs of other criminal groups globally.

Pacific Island Countries and Territories

Authorities in and around the Pacific region have increasingly reported that major transnational criminal networks centred in Southeast Asia are among the most active across the Pacific Island Countries and Territories (PICTs).[5] These networks have steadily expanded power and influence in the region, with a growing number of incidents beginning in 2017 indicating they have targeted the tourism and entertainment industries of select Pacific Islands.



Suspected trafficking in persons victims detained following raids on illegal online gambling operations housed in hotels linked to senior members of the 14K Triad in Palau. Source: Office of the Special Prosecutor of Palau, 2020.

5 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*, October 2024.

Similarly to their approach across Southeast Asia, transnational organized crime groups operating in the Pacific have built up their footholds through the development of casinos, junkets, hotel resorts, travel agencies, and other related businesses and investment projects, often involving virtual assets. This modus operandi has proven highly effective in concealing and facilitating various illicit activities including illegal online gambling, drug trafficking, human trafficking, migrant smuggling, and money laundering which have spiked in certain parts of the region.[6] Signs of related criminal activities and operations linked to organized crime have recently been observed in PICTs including Fiji, Palau, Samoa, Tonga, Vanuatu, and the Commonwealth of the Northern Mariana Islands (CNMI), with most challenged by limited human and technical resources facing significant difficulties in detecting and disrupting these activities.[7]



Grand Mariana Casino Hotel and Resort Saipan developed by criminally implicated Imperial Pacific International Holdings. Source: Imperial Pacific International, 2024.

For this reason, Asian crime syndicates operating in the Pacific have been able to do so very openly, with some senior members appearing in public and presenting themselves as legitimate foreign investors in sectors that can be useful for their illicit businesses. Leaders of these networks have effectively formed alliances with influential local figures, leveraging these relationships, alongside mutual financial interests, to advance business interests and spread influence. Criminal groups operating in the pacific have also exploited citizenship-by-investment (CBI) schemes, particularly in Vanuatu, which has been documented being offered as a service, among CBI schemes in other countries, to networks operating within Southeast Asia-based scam centres.[8]

6 Ibid.
7 Ibid.
8 Ibid.

Africa

While many African countries have long faced challenges related to their own indigenous cyber enabled fraud and scam industries, in recent years there have been increasing indications of major Asian criminal networks establishing connections and operations on the continent and exploiting similar vulnerabilities to those present in Southeast Asia.

Beginning in early 2024, reports started to emerge of significant operations being identified by law enforcement across Africa. For instance, in April 2024, a fraud syndicate was discovered in Zambia, leading to the arrest of 77 suspects, including 22 Chinese nationals who were later sentenced to up to 11 years in jail for leading the operation.[9] In late 2024, there were also reports of significant raids in Angloa, where dozens of Chinese nationals were detained for alleged involvement in online gambling, fraud, and cybercrime,[10] while another alleged 'pig butchering' operation was also dismantled in Namibia in late 2023, with authorities arresting a mix of Chinese, Cuban, Namibian, and Singaporean nationals.[11]



Suspects held after arrest in Lagos, Nigeria. Source: Economic and Financial Crimes Commission, December 2024.

Nigeria has notably emerged as an important destination for Asian fraud networks diversifying into Africa. Two major raids occurred in December 2024 and January 2025 in Lagos and Abuja, respectively, leading to the arrest of nearly 1,000

9 Drug Enforcement Commission of Zambia, April 2024.
10 Angola24horas, "Chineses detidos em Luanda por gestão fraudulenta de mais 400 jogos 'online'", 28 August 2024, available at: https://angola24horas.com/sociedade/item/30310-chinesesdetidos- em-luanda-por-gestao-fraudulenta-de-mais-400-jogosonline; Angop, "National Police arrest social media scammers in Luanda", 21 October 2024, available at: https://angop.ao/en/ noticias/sociedade/detidos-cidadaos-chineses-por-criacao-deperfis- falsos-para-burlas-nas-redes-sociais/.
11 Werner Menges, "PG reveals details of 'pig butchering' online crypto investment scam", The Namibian, 28 January 2025, available at: https://www.namibian.com.na/fake-social-mediaaccounts- revealed-in-crypto-scam/.

people.[12] Among them were hundreds of foreign nationals from East and Southeast Asia suspected of involvement in cryptocurrency investment and romance scams. The Economic and Financial Crimes Commission (EFCC) stated that the foreign nationals trained Nigerian accomplices, demonstrating the corrupting influence of the industry and signaling the potential of significantly expanding collaboration between Asian and Nigerian criminal groups.[13]

Indication of further expansion

South America

Recent trends and incidents indicate that transnational organized crime groups from Asia have increasingly expanded into and targeted various parts of South America. While data remains limited in comparison to other regions, Asian criminal networks have been observed scaling up their South American-facing online operations and infrastructure.[14] This has been particularly noticeable in the case of cyber-enabled fraud and illegal online gambling platforms in past years, leading to a parallel increase in demand for Spanish and Portuguese speaking labour within Southeast Asian scam centres.[15] These crime groups have also sought to enhance critical money laundering and underground banking partnerships with major South American drug trafficking organizations or cartels and, in a number of isolated cases, have managed to establish physical scam operations locally.



Rescued Malaysian victims and Red Dragon gang members detained by Peruvian authorities. Source: Peruvian National Police, October 2023.

12 Economic and Financial Crimes Commission, "EFCC Bursts Syndicate of 792 Cryptocurrency Investment, Romance Fraud Suspects in Lagos … Arrests 193 Chinese, Arabs, Filipinos, Others", 16 December 2024, available at: https://www.efcc.gov.ng/ efcc/news-and-information/news-release/10584-efcc-burstssyndicate- of-792-cryptocurrency-investment-romance-fraudsuspects- in-lagos-arrests-193-chinese-arabs-filipinos-others

13 Ibid.

14 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.*

15 Japan National Police Agency, "Global Fraud Meeting", September 2024.

South Asia

South Asian nations have also been increasingly impacted by the evolving situation and spillover in Southeast Asia. While countries in the region have long served as a base for call centre scam operations, as the industry grew in Southeast Asia, it has become increasingly targeted by neighbouring cyber-enabled fraud industries as both a source of revenue and labour. This is reflected in the large number of Indian and other South Asian nationals repatriated from scam centres in Myawaddy, Myanmar, in March 2025, as well as other large-scale efforts by the Indian Government to extract nationals from compounds in Lao PDR and Cambodia.[16] Raids and rescues across Southeast Asia have also identified nationals of Bangladesh, Bhutan, Nepal, Pakistan, and Sri Lanka.

It is worth noting that Sri Lanka has also shown signs of being targeted as a base of criminal operations. In 2024, several raids led to the arrest of hundreds of people, including Chinese, Filipino, Indonesian, Malaysian, Thai, and Vietnamese nationals found at suspected cyber-enabled fraud operations, providing further evidence of spillover beyond Southeast Asia.[17]

Emergence of new illicit online marketplaces and integrated money laundering services

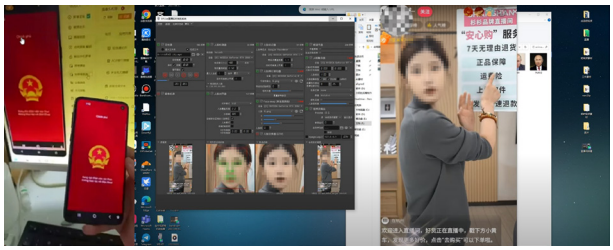
Significant developments relating to illicit online marketplaces servicing transnational criminal groups in Southeast Asia have taken place over recent years, exacerbating existing challenges and impacts in and beyond the region. Several platforms controlled by powerful criminal networks have come to dominate the regional illicit economy, serving as a key catalyst behind rapid ongoing expansion and the industry's increasing global impact.

This development has fundamentally revolutionized the business model for transnational organized crime based in Southeast Asia, resulting in a surge of specialized service providers entering the market and supporting illicit industries. Leading marketplace platforms have integrated cryptocurrency and other financial services often controlled by the same or other adjacent

16 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, *p.48.*

17 Sri Lanka Police Service, "Official Media Statements", October 2024.

criminal networks, hosting a range of merchants specializing in the sale of fraud kits, stolen data, malware, AI-driven tools, and various underground banking, money laundering and cybercrime services utilized by other criminals targeting victims globally. These online platforms actively present themselves as legitimate, registered businesses and 'neutral third parties' often affiliated with larger business networks. However, most are wholly unauthorized to engage in online payment processing, cryptocurrency trading and exchange, and other related activities, operating with little to no regulatory oversight.

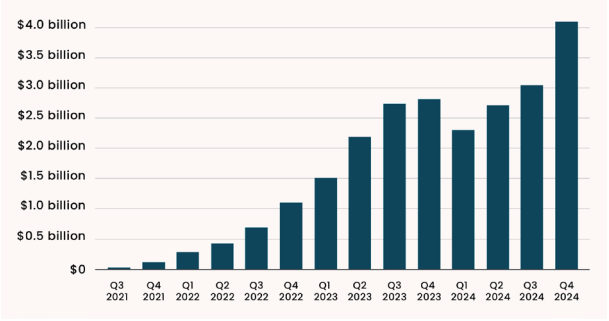


Screen capture of demos shared by malware and deepfake software vendors advertising solutions to Mekong-based criminal groups engaged in police impersonation fraud identified by ChongLuaDao (Viet Nam) and UNODC researchers, 2024.

According to several studies, Huione Guarantee, recently rebranded Haowang,[18] has emerged as one of the world's largest illicit online marketplaces by users and transaction volume, representing a key piece of infrastructure driving cyber-enabled fraud in Southeast Asia.[19,20] Headquartered in Phnom Penh, Cambodia, the predominantly Chinese-language platform has grown to more than 970,000 users and thousands of interconnected vendors at the time of writing. It is linked to subsidiaries registered in countries including Canada, Poland, Hong Kong, China, and Singapore, and has also registered trademarks currently active in the United States and elsewhere.[21]

Huione Guarantee has processed tens of billions of dollars in cryptocurrency transactions since 2021, with on-chain analysis indicating that the platform has become a one-stop-shop for illicit actors sourcing the technology, infrastructure, data, and other resources needed to conduct cyber-enabled fraud and cybercrime, as well as large-scale money laundering and sanctions evasion. Some expert estimates have found that cryptocurrency wallets used by Huione Guarantee and its vendors have received inflows totaling at least US $24 billion over the past four years,[22] with law enforcement authorities and blockchain researchers reporting clear connections between the marketplace and criminal groups targeting victims around the world.

Figure 2. Value of cryptocurrency inflows received by wallets used by Huione Guarantee and its vendors, 2021 - 2024



Source: Elliptic, 2025.

Concerningly, Huione has recently launched a range of its own cryptocurrency-related products including a cryptocurrency exchange and trading application, online gambling platform, blockchain network, and US Dollar-backed stablecoin designed to circumvent government controls. A growing number of Huione Guarantee vendors have also shown increasing signs of specialization within certain in-demand jurisdictions outside of Southeast Asia in response to shifting market needs, with several high-profile cases highlighting the platform's intensifying global impact.

Amidst heightened awareness and scrutiny, several competing entities with known criminal ties have been observed expanding their virtual asset service businesses and establishing similar Guarantee-style platforms on Telegram, indicating that any significant efforts to disrupt existing platforms are likely to be offset by others emerging within the region.

18 Huione Guarantee has tried to distance itself from Huione Group. For example the marketplace recently renamed itself to "Haowang Guarantee". Huione Group's payments business, Huione Pay also removed a section on its website dedicated to the marketplace and describing Huione Guarantee as a subsidiary. Despite this superficial distancing, Huione Guarantee confirmed that Huione Group remains a "strategic partner and shareholder".

19 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*

20 Elliptic, "Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin", January 2025, available at: https://www.elliptic.co/blog/huione-largest-everillicit- online-marketplace-stablecoin.

21 United States Patent and Trademark Office database, April 2025.

22 Elliptic, "Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin", January 2025, available at: https://www.elliptic.co/blog/huione-largesteverillicit- online-marketplace-stablecoin.

Recommendations

The following recommendations are intended to support countries in Southeast Asia — particularly those in the Mekong subregion — in addressing the key vulnerabilities identified in this report, and ultimately to strengthen the awareness, understanding, and capacity of governments, oversight authorities, and law enforcement in Southeast Asia, and particularly those in the Mekong region. They build on targeted recommendations informed by ongoing dialogues and consultations with governments and law enforcement in the region, and are aligned with comprehensive and strategic recommendations agreed under the *ASEAN + China Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia*.[23]

Each priority area set out below addresses a distinct dimension of the response, while reinforcing the others. This approach is designed to be modular and scalable, enabling countries to adapt interventions to their specific national context while contributing to a unified and coordinated regional strategy.

Raising political awareness and will

Sustained political commitment is essential to elevating scam centres and associated organized crime and corruption as national and regional security concerns. Addressing these threats requires clear recognition at senior levels of government and coordinated messaging across relevant institutions.

- High-level engagement is needed to acknowledge the strategic impact of scam operations and transnational organized crime.
- Raising awareness across government, private sector, and civil society enhances understanding of the risks posed by cyber-enabled fraud, underground banking, and illicit financial flows.
- National and regional platforms provide opportunities for dialogue, coordination, and collective priority-setting.
- Public education and outreach initiatives help increase understanding of the enabling role of casinos, virtual assets, and other high-risk sectors.
- Criminalizing corrupt acts and enhancing other measures to address and prevent corruption, including by encouraging reporting and protecting reporting persons.

Strengthening regulatory frameworks

Effective prevention and enforcement depend on well-designed legal and regulatory systems that can respond to evolving threats. Closing legislative gaps and aligning frameworks with international standards will help limit the opportunities for criminal exploitation.

- Legal frameworks addressing money laundering, virtual assets, SEZ and casino oversight, and online gambling benefit from periodic review and reform.
- Oversight mechanisms should be applied to financial flows and investment activities in high-risk sectors such as special economic zones and junkets.
- Licensing and supervisory tools are essential for monitoring high-risk financial service providers, particularly those operating through digital platforms.
- Legal provisions that facilitate investigation, prosecution, and asset recovery—while safeguarding victims—strengthen institutional resilience.

Enhancing the technical and operational capacity of enforcement agencies

Enforcement agencies need the tools, skills, and systems required to detect, investigate, and disrupt transnational organized crime. Building institutional capacity and ensuring access to appropriate resources will improve the effectiveness of frontline responses.

- The ability to monitor and investigate threats such as cyber-enabled fraud, underground banking, and misuse of virtual assets should be continuously developed.
- Financial and digital evidence must be collected, preserved, and analyzed in ways that strengthen the integrity of investigations and prosecutions.
- Reducing reliance on victim testimony in

23 UNODC, ASEAN Member States and the People's Republic of China Regional Cooperation Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia, September 2023, available at: https://www.unodc.org/roseap/2023/09/asean-china-action-plan-criminal-scams/story.html.

trafficking cases through improved investigative techniques is essential to victim-centred justice.
- Specialized training, inter-agency collaboration, and appropriate technology all contribute to stronger enforcement outcomes.

Promoting whole-of-government responses and inter-agency coordination

An integrated national response requires collaboration among all relevant institutions involved in prevention, enforcement, regulation, and protection. Effective coordination mechanisms can bridge institutional silos and improve decision-making.

- National coordination bodies can bring together relevant ministries, enforcement agencies, and oversight institutions.
- Joint training and planning processes improve coherence and shared understanding across sectors.
- Identification, protection, and referral systems for victims of forced criminality should be strengthened and consistently applied.
- Strengthen oversight of border management and accountability for border officials who facilitate trafficking for forced criminality, as well as those who provide protection to scam centres.
- Cooperation among countries of origin, transit, and destination is vital to support safe return, reintegration, and continued assistance for victims.

Advancing practical and operational regional cooperation

Cross-border cooperation is essential to address the transnational nature of scam operations and associated criminal infrastructure. Collective efforts can help prevent displacement, share intelligence, and support enforcement across jurisdictions.

- Mechanisms for timely information exchange and operational coordination should be reinforced at bilateral and regional levels.
- Regional platforms offer a basis for joint investigations and collaboration on high-priority cases.
- Shared research and typology development to improve situational awareness and guide risk-based responses.
- Engagement with multilateral frameworks strengthens mutual legal assistance and supports coordinated approaches beyond the region.



Report development and analysis



Report development and analysis

The present report is part of a growing body of threat analyses conducted by UNODC on transnational organized crime in Southeast Asia.

In 2019, UNODC released the report *Transnational Organized Crime in Southeast Asia: Evolution, Growth, and Impact,* which provided a comprehensive analysis of the characteristics and evolution of organized crime, including various forms of trafficking, over a five-year period. The report also identified key vulnerabilities in the region, such as drug trafficking and associated money laundering activities, particularly in border regions that have witnessed the growth of casinos and Special Economic Zones (SEZs).

The findings of the report were presented to policymakers, law enforcement agencies, international partners, academics, and other experts, with the objective of fostering dialogue and advancing efforts to address organized crime more effectively. Subsequently, in November 2019, UNODC engaged with Ministers and senior officials from Cambodia, China, Lao PDR, Myanmar, Thailand, and Viet Nam, under the framework of the Mekong Memorandum of Understanding on Drug Control, where a new political framework and action plan were agreed upon to address the escalating drug situation. A targeted policy brief on casinos and money laundering served as a basis for these discussions, which resulted in consensus on the need for a deeper examination of the connections between organized crime, drug trafficking, money laundering, and casinos and SEZs in the region.

Other countries in the region also expressed support for this initiative, recognizing the necessity of a study that would explore the interplay between the casino industry, money laundering, drug trafficking, and transnational organized crime, to better equip regional governments with the tools for multilateral cooperation and strategic responses. Against this backdrop, the proliferation of large-scale cyber-enabled fraud operations, often integrated within casinos and SEZs, was also flagged as an urgent and growing concern by some Member States.

UNODC proceeded to initiate an internal assessment focusing on casinos, money laundering, and transnational organized crime in Southeast Asia, alongside a separate analysis of illicit financial flows. This research was carried out by a team of in-house analysts and international experts, in consultation with an extensive network of regional security, law enforcement, and financial intelligence agencies. The analysis provided a detailed overview of the major threats and risks associated with the proliferation of casinos and the sophisticated money laundering methods employed by organized criminal groups. One of the most significant findings was the rapid shift of criminal operations online, exacerbated by the COVID-19 pandemic and increased regulatory scrutiny. This trend was especially evident in the rise of underregulated illegal online gambling platforms, e-junkets, and cyber-enabled fraud, which has fundamentally altered the criminal landscape in Southeast Asia.

In expanding on this work, UNODC initiated a series of bilateral and multilateral meetings with law enforcement, financial intelligence units, and casino regulatory bodies to monitor the evolving situation, particularly concerning online casinos, junkets, and known organized crime groups. Due to the sensitivity of the information, many of these meetings were conducted in confidential settings over the course of more than a year. Simultaneously, UNODC undertook a comprehensive review of criminal indictments, case files, financial intelligence reports, and court records, culminating in a detailed threat assessment titled *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*, which was published in January 2024.

In October 2024, UNODC published an immediate follow-up threat analysis building on these findings alongside new information and data highlighting the evolving nature of the situation and various shifting dynamics brought on by rapid technological advancement. Titled *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, the analysis relied heavily on information and intelligence shared with UNODC throughout an ongoing series of closed-door gatherings of regional analysts and investigators.

The present report builds on this ongoing body of work, taking into account the intensifying global impacts and implications of the ongoing situation and recognizing that the international community now stands at a critical inflection point. UNODC has maintained a vigilant approach to tracking the evolving threat landscape, convening regional authorities and international partners in closed-door settings to enhance the exchange of critical information and intelligence. This effort has guided law enforcement and policy strategies, ultimately culminating in the development of this study. Extensive data and information produced by national and regional authorities as well as civil society and international organizations and private sector partners within the blockchain, cybersecurity, and iGaming industries were also reviewed. This includes a variety of corporate records and other filings related to casinos, virtual asset service providers, and confirmed scam centres in the region, drawing from sources across East and Southeast Asia, Australia, Canada, Europe, India, the United Kingdom, and the United States, among others. Official case information and other related data used for this study were also compiled by various UNODC field offices across Africa, Latin America, and the Middle East, as well as UNODC's regional working group on illicit financial flows and emergency response network (ERN).

To ensure a thorough understanding of the landscape, UNODC employed advanced techniques, conducting an extensive analysis of near real-time data from thousands of Telegram underground marketplaces, groups and channels attributed to Asian organized crime networks and affiliated service providers, leveraging aggregated quantitative analysis and multi-lingual keyword monitoring. This effort, supported by retrieval augmented generation (RAG) and qualitative analysis, extended to various clear web and dark web platforms, forums, and marketplaces used for a wide range of illicit activity relating to cyber-enabled fraud, drug trafficking, human trafficking and migrant smuggling, and related underground banking and money laundering in the region.

This report examines both primary and secondary data points and pulls them into the context of UNODC's prior analysis and understanding of organized crime in Southeast Asia, aiming to enhance awareness of the scope of the challenge and support regional governments in addressing it. It outlines key vulnerabilities, threats, and risks related to the integration of technological advancements into the regional criminal ecosystem, and the growing professionalization this has brought. It also provides a series of recommendations intended to assist governments and international partners to better deal with the fast-evolving issues involving casinos and organized crime in Southeast Asia.

The findings should serve as a foundation for future threat monitoring and analyses, and drive solutions- oriented dialogue about the convergence of cyber-enabled fraud, underground banking, and technological innovation, and will be used as a basis for future discussions, ongoing technical assistance, and the development of response strategies with authorities across the region.



Regional overview



Regional overview

Introduction

Transnational organized crime groups in East and Southeast Asia have emerged as global market leaders in cyber-enabled fraud, money laundering and underground banking. These groups have grown exponentially in recent years, demonstrating the ability to utilize and adapt to changes in political and business environments, exploit gaps in governance and regulations, and rapidly develop physical, information, communication, and blockchain infrastructure while integrating new business models and technologies including malware, artificial intelligence, and deepfakes into their operations.

Amidst heightened awareness and enforcement action taken to address the proliferation of industrial-scale scam centres by governments in the region, Asian crime syndicates have sought to hedge their risk and ensure business continuity by expanding operations deeper into many of its most remote, vulnerable, and underprepared parts. The dispersal of these sophisticated criminal networks within areas of weakest governance has attracted new players, fueled corruption, and enabled the illicit industry to continue to scale and consolidate, culminating in hundreds of industrial-scale scam centers generating tens of billions of dollars in annual profits according to latest estimates.[1]

In the United States alone, authorities reported more than US $5.6 billion in financial losses to cryptocurrency scams in 2023, with an estimated US $4.4 billion attributed to so-called 'pig butchering' schemes most prevalent in Southeast Asia.[2] Regionally, countries in East and Southeast Asia combined have lost up to an estimated US $37 billion during that same year according to latest available data.[3]

Like any business, transnational criminal enterprises seek out conditions that ensure continuity of business with limited government interference. In so doing, these actors have converged around special economic zones, casinos, resorts and hotels, and remote border areas, as well as several non-state armed group-controlled special or autonomous regions, to house their operations. As the industry expanded, purpose-built business parks were developed to house and service online crime operations. These venues and businesses have proven to offer a highly protected operating environment conducive to organized crime, featuring all of the conditions, infrastructure, and regulatory, legal, and fiscal covers required for sustained growth and expansion. More than this, it is apparent when considering the totality of the situation that the region has essentially become an interconnected ecosystem within which organized crime syndicates exploit vulnerabilities, jeopardize state sovereignty, and distort and corrupt policy-making processes and other government systems.

1 UNODC, "Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape", October 2024.

2 Federal Bureau of Investigation, "Internet Crime Complaint Center, Cryptocurrency Fraud Report", 2023, available at: https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf.

3 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*.

Against this backdrop, many of the region's largest criminal groups that have expanded and consolidated their bases of operation in the region have increasingly diversified their business lines towards the development of key infrastructure. This has extended far beyond the construction and management of physical scam compounds to include unlicensed and high-risk online gambling platforms, payment processors, cryptocurrency exchanges, stablecoins,[4] blockchain networks, encrypted communications platforms, and illicit online marketplaces, often controlled by the same actors, compounding existing law enforcement challenges and fueling industry growth.

As evidenced by the increasingly global range of services on offer by criminal actors across numerous Telegram-based illicit online marketplaces and forums native to Southeast Asia, it is also apparent that recent developments in the region have incentivized a growing number of criminal networks to hedge beyond it. This trend has been consistent with continued reports of crackdowns targeting Asian-led overseas cyber-enabled fraud operations with major ties to networks based in Southeast Asia, including those found operating in Africa, South Asia, the Middle East, and select Pacific islands, as well as related money laundering, trafficking in persons, and recruitment services as far as Europe, North America, and South America.

Many of these groups have now managed to take on industrial proportions by reinvesting their profits and leveraging vast multi-lingual workforces comprised of hundreds of thousands of trafficked victims and complicit individuals. This has rapidly enabled organized crime based in Southeast Asia to broaden the scope of fraud victims being targeted globally, with virtually no jurisdiction left immune. At the same time, the ongoing expansion has created new needs, opportunities, and strengthened partnerships between globalized Asian crime syndicates and a growing number of overseas criminal groups – a trend which has been particularly documented in the area of money laundering and underground banking. This has not only fueled further expansion of the criminal ecosystem across Southeast Asia and other parts of the world, but has simultaneously driven up demand for new high-speed channels capable of integrating billions in criminal proceeds into the formal financial system undetected.

4 Stablecoins are cryptocurrencies pegged to and backed by fiat currencies such as the U.S. Dollar.

The following section outlines key developments and trends within the regional organized crime ecosystem and its intensifying global impact, examining vulnerabilities that continue to enable its self-sustained growth, and why the present situation has reached a critical inflection point which must be recognized as a serious, evolving transnational security concern.

Building pressure against key online crime sites

As cyber-enabled fraud and other illicit online industries established themselves in Southeast Asia, they have developed deep roots and expanded exponentially. Criminal networks have become entrenched in certain areas in a relatively short period, and the industry has also become known for its extreme mobility and adaptability. Over the past two years, law enforcement actions have targeted online operations in Cambodia, the Philippines, Lao PDR, Myanmar, and Thailand. These actions have varied in their scope and duration, but all have resulted in responses from the industry.

With respect to policy and law enforcement developments in the region, one of the largest crackdowns in Southeast Asia has taken place in eastern Myanmar, focusing largely on Myawaddy and surrounding areas along the Thai-Myanmar border. This followed recent bilateral engagements between China's Ministry of Public Security and its counterparts in both Thailand and Myanmar, which culminated in the suspension of cross-border power transmission and sales of fuel in early 2025. Following action by the Thai Government, non-stated armed groups in control of key border territories from which online crime groups operate have conducted targeted inspections of several well-known sites, and in the weeks following several thousand people were handed to Thai authorities on the border (returned to below).[5]

This was the first crackdown of this scale implemented in eastern Myanmar, but follows on from major operations that occurred in the north beginning in late 2023.[6] Operations commenced in Wa State in September 2023, when authorities

5 Royal Thai Police, "Stakeholder Roundtable Dialogue", February 2025.

6 For more information, see: UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, p.52-55.

initiated a crackdown on the industry, followed soon after by the launch of law enforcement action in the Kokang Self-administered Zone, which was soon overtaken by a major military offensive by ethnic armed groups that removed the Kokang Border Guard Force and scattered online operators. According to China's Ministry of Public Security, over 50,000 Chinese nationals were detained in northern Myanmar and repatriated by January 2024.[7]

As part of the initiative, in November 2023, China's public security organs issued wanted notices for four members of the Ming family, which was described as a "telecom network fraud criminal group".[8] The following month notices were issued for 10 more key players in the Kokang region who held administrative, military and police positions, while also leading major transnational conglomerates implicated in online crimes,[9] including members of the powerful Bai, Wei and Liu families.[10] Members of the Ming family were handed over to China in November, and in early 2024 another 10 alleged crime group leaders were handed over, including six of those subject to earlier wanted notices. The trial of the arrested Ming family members and associates began in Wenzhou, China, in February 2025. A total of 23 defendants face charges including fraud, intentional homicide, intentional injury, illegal detention, extortion, opening illegal casinos, organizing prostitution, drug trafficking, and organizing others to illegally cross a national border.[11]

Law enforcement action has continued in the north of Myanmar, albeit not with the same intensity as in late 2023 to early 2024. For example, in November 2024, Wa State handed over 762 Chinese nationals to counterparts on the border after the United Wa State Army raided scam operations in Tangyan.[12] Wa State authorities report frequently on other arrests and deportations, often involving smaller groups of 10-20 people.[13] Myanmar's State Administration Council (SAC) – the official name of Myanmar's current military authorities – has also reported raids in other parts of Shan State, with over 100 arrested in raids in Shan State in February of 2025.[14]



Members of the Ming family handed over to Chinese police. Source: Criminal Investigation Bureau of the Ministry of Public Security of the People's Republic of China, 2023.

7 Criminal Investigation Bureau of the Ministry of Public Security of the PR China, "Ministry of Public Security: In recent years, more than 50,000 fraud suspects have been arrested in northern Myanmar", 27 August 2024, available at: https://mp.weixin.qq.com/s/SZTsIgEwAeTgZ9XHQkCtA.

8 Criminal Investigation Bureau of the Ministry of Public Security of the PR China, "The public security authorities have publicly issued a wanted notice for Ming Xuechang, Ming Guoping, Ming Julan and Ming Zhenzhen, four important leaders of the telecommunications and Internet fraud criminal group in Kokang Self-administered Zone in northern Myanmar", 12 November 2023, available at: https://mp.weixin.qq.com/s/3_0nZUBvMeM37Xkf0u0U3A.

9 Criminal Investigation Bureau of the Ministry of Public Security of the PR China, "The public security organs have publicly issued a wanted notice for Bai Suocheng, Wei Huairen, Liu Zhengxiang and 10 other important leaders of the telecommunications and Internet fraud criminal group in Kokang Self-administered Zone in northern Myanmar", 10 December 2023, available at: https://mp.weixin.qq.com/s/sm3wSWuxPSFcuSg4zlEfsQ.

10 Wanted notices were issued for Bai Suocheng (former chairman of Kokang region), Bai Yingcang (head of a Kokang militia, deputy director of Kokang Economic Development Bureau, and chairman of the Cangsheng Science & Technology Park), Bai Yinglan (chair of the Xinbaili group), Wei Huairen (head of a border battalion supervision committee, Wei Qingsong (member of the same border committee), Wei Rong (chair of Hengli Group), Liu Zhengxiang (director of Kokang Urban Development Bureau and chair of Fulilai Group), Liu Jiguang (director of the Kokang Health Bureau and executive director of Fulilai Group), Liu Zhengmao (general manager of Fulilai Group), and associate Xu Laofa.

11 Criminal Investigation Bureau of the Ministry of Public Security of the PR China, "The first trial of the Ming Family criminal group case begins", 19 February 2025, available at: https://mp.weixin.qq.com/s/uwPHS12Fj1PQiivdNlIDWg.

12 Wa State Police, "Military and police work together to act quickly! Wa State handed over 762 Chinese nationals involved in fraud to China", 20 November 2024, available at: https://mp.weixin.qq.com/s/onz2ztC06RaopCJcCRdy1Q.

13 For example, see: Wa State Police, "Wa State Judicial Committee handed over 20 Chinese nationals involved in the case to China", 11 January 2025, available at: https://mp.weixin.qq.com/s/vgBzI3JoikdkFaKKPI-CLw.

14 Myanmar State Administration Council Ministry of Information, "Those involved in illegal online gambling and money laundering (scams) in Mong Ha area of Mong Ye Township, Shan State (Northern) will be identified and arrested, necessary investigations will be conducted, and the suspects will be transferred to the relevant countries", 7 February 2025, available at: https://myanmar.gov.mm/news-media/-/asset_publisher/Jb7SCMXVsWI1/content/%25E1%2580%259B%25E1%2580%25BE%25E1%2580%2599%25E1%2580%25BA%25E1%2580%25B8%25E1%2580%2595%25E1%2580%25BC%25E1%2580%258A%25E1%2580%25BA%25E1%2580%2594%25E1%2580%259A%25E1%2580%25BA-%25E1%2580%2599%25E1%2580%25BC%25E1%2580%25B1%25E1%2580%25AC%25E-72.

Elsewhere, in the Philippines, authorities are currently implementing a ban on Philippine Offshore Gambling Operators (POGOs)[15] that came into force in November 2024.[16] After being formalized in 2016, POGOs established huge multi-building complexes, with the industry employing hundreds of thousands of foreigners and Filipinos at its peak. Despite being established explicitly to regulate offshore online gambling operations, the POGO system became highly controversial due to its inability to cope with widespread criminality.[17] Investigations uncovered criminal networks operating under the cover of POGOs, many of which housed transnational criminal groups engaged in a wide array of illicit activities, including cyber-enabled fraud, trafficking in persons, kidnapping, extortion, and groups providing cybercrime and professional money laundering services, with some implicated in major global money laundering investigations.[18]

After the ban was issued in November, POGO operators were instructed to wind up operations and foreign employees told to leave the country. Many ceased operations and immigration authorities reported more than 20,000 POGO workers left the country, but law enforcement activities targeting illegal operations continued. Raids have taken place across the country, including in Davao del Norte, Parañaque, Cavite, Manila, Makati, and others. Despite the ban, there are indications that major operations are still active, including one action in Parañaque in January 2025 which led to the apprehension of 400 foreigners, who were detained by immigration authorities awaiting deportation.[19] Another raid in Parañaque the following month apprehended over 450 people, a third of whom were foreigners.[20]

Hundreds of people detained in such raids have been deported in recent months, including 187 Chinese nationals involved in illegal online gaming operations in Pasay City and Cebu who were deported in December.[21] According to the Presidential Anti-Organized Crime Commission (PAOCC), by the end of 2024, over 2,300 people who worked for offshore gaming operators shut down by law enforcers had been deported, mostly to China.[22,23] Hundreds more have already been deported in 2025.

In Lao PDR, the Golden Triangle Special Economic Zone (GTSEZ) has long been associated with transnational crime networks, and is a well-documented site for drug trafficking, illegal wildlife trade, trafficking in persons, money laundering, online gambling and cyber-enabled fraud. In 2018, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned GTSEZ founder, Zhao Wei, and several of his companies and associates, alleging he was the mastermind of a 'transnational criminal organization'.[24] Between 2022 and 2023, Zhao and several associates have also obtained Cambodian citizenship under which they now control numerous property and investment holdings, including islands off the coast of Sihanoukville obtained through 99-year property development concessions.[25]

15 Platforms targeting overseas gamblers were legalized in 2016 and licensed as Philippine Offshore Gambling Operators (POGOs). POGOs established huge multi-building complexes, known in some cases as POGO hubs, with the industry employing hundreds of thousands of foreigners and Filipinos at its peak. Despite being established explicitly to regulate offshore online gambling operations, the POGO system proved highly controversial due to its inability to cope with widespread criminality.

16 The President of The Philippines, "Executive Order No. 74: Immediate Ban of Philippine Offshore Gaming, Internet Gaming, and Other Offshore Gaming Operations in The Philippines, and for Other Purposes", 5 November 2024, available at: https://www.officialgazette.gov.ph/2024/11/05/executive-order-no-74-s-2024/.

17 UNODC, "Roundtable on Transnational Organized Crime, Online Gambling and Cyber-Enabled Fraud", Manila, Philippines, May 2024.

18 For a discussion of action targeting POGOs and a list of major raids in 2023-24, see: UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, p.36-37, 50-51.

19 Philippines Bureau of Immigration, "BI Arrests almost 400 Illegal Aliens in Major Raid on alleged Scam Operations in Paranaque", 8 January 2025, available at: https://immigration.gov.ph/bi-arrests-almost-400-illegal-aliens-in-major-raid-on-alleged-scam-operations-in-paranaque/.

20 Philippines Bureau of Immigration, "BI Commends POACC for new arrest, vows tighter coordination against illegal POGOs", 23 February 2025, available at: https://immigration.gov.ph/bi-commends-poacc-for-new-arrest-vows-tighter-coordination-against-illegal-pogos/.

21 Philippines Bureau of Immigration, "BI Deports 187 illegal POGO workers arrested with PAOCC", 06 December 2024, available at: https://immigration.gov.ph/bi-deports-187-illegal-pogo-workers-arrested-with-paocc/.

22 Philippines Information Agency, "No more POGOs in Bagong Pilipinas", 04 March 2025, available at: https://pia.gov.ph/no-more-pogos-in-bagong-pilipinas/. https://globalnation.inquirer.net/258113/philippines-deports-2300-pogo-workers-to-china-other-asian-countries/

23 Philippines Presidential Anti-Organized Crime Commission, "Press Statement", March 2025.

24 U.S. Department of the Treasury, "Treasury Sanctions the Zhao Wei Transnational Criminal Organization", 30 January 2018, available at; https://home.treasury.gov/news/press-releases/sm0272.

25 Ministry of Commerce of Cambodia, "Online Business Registration Portal", available at: https://www.businessregistration.moc.gov.kh/



Islands under development by OFAC sanctioned Zhao Wei and associates. Source: Ministry of Commerce of Cambodia, Online Business Registration Portal and Google Earth.

Joint law enforcement action targeting online crime operations in the GTSEZ in Lao PDR began to increase in 2023 and 2024, culminating in a series of highly publicized raids across the zone and the arrest of hundreds of mostly foreign nationals. Following a major operation which resulted in the arrest of more than 700 people in August 2024,[26] inspections targeting cyber-enabled fraud operations began to intensify across the zone, although there is limited detail available on the outcomes of these inspections, reports indicate further arrests were made. However, instructions from the SEZ Management Board Committee indicate companies operating in the zone have been pushed to centralize their operations. According to media reports, the 16 companies reportedly licensed to operate online gaming were told in November 2024 to relocate their 95 subsidiaries to the same building or neighbourhood to streamline oversight.[27] There is, however, no publicly available register of companies that have received online gaming licenses in Lao PDR, making it difficult to assess the extent to which enforcement actions in 2024 have had an impact.

While there have been sporadic raids in Cambodia targeting online crime sites in Phnom Penh, Bavet and Poipet, there has been no widely publicized 'campaign' style law enforcement drive since a series of raids that largely focused in Sihanoukville in 2022. However, the Cambodian Government has continued to state its commitment to tackling the issue, and in February 2025 announced the formation of a new task force for combatting online scams, including high-level officials from across government and headed by the prime minister.[28]

Increased external pressure has targeted the industry, and in 2024 the United States Department of the Treasury's OFAC sanctioned Senator Ly Yong Phat and two of his companies for their role in "serious human rights abuse related to the treatment of trafficked workers subjected to forced labor in online scam centers", specifically highlighting known locations of online gambling and cyber-enabled fraud in Oddar Meanchey and Koh Kong provinces.[29] The Cambodian Government expressed 'deep regret' in response to the sanctions, and branded them 'politically motivated'.[30]

In response to law enforcement actions in various jurisdictions, criminal networks have pivoted, sometimes moving entire operations to new locations, dispersing into smaller cells, or rebranding by changing their operational cover. When there have been disruptions to the infrastructure and services they depend on, such as internet connection or power supply, they have found alternatives that have enabled them to continue. As will be explored later in the report, the platforms that have been established to receive, launder and move funds have also adapted to increasing attention and disruption from global law enforcement agencies.

26 For more details, see: UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, p.50-52.

27 Laotian Times, "Bokeo Tightens Control on Online Gaming Firms to Curb Cyber Fraud", 7 November 2024, available at: https://laotiantimes.com/2024/11/07/bokeo-cracks-down-on-telecom-cyber-fraud-in-special-economic-zone/.

28 Royal Government of Cambodia, "Decision on the Establishment of the Commission on Combatting Technology Fraud (Online Scams)", 20 February 2025.

29 U.S. Department of the Treasury, "Treasury Sanctions Cambodian Tycoon and Businesses Linked to Human Trafficking and Forced Labor in Furtherance of Cyber and Virtual Currency Scams", 12 September 2024, available at: https://home.treasury.gov/news/press-releases/jy2576.

30 Ministry of Foreign Affairs and International Cooperation, Statement by the Ministry of Foreign Affairs and International Cooperation, 13 September 2024, available at: https://www.mfaic.gov.kh/posts/2024-09-13-Press-Release-Statement-of-the-Ministry-of-Foreign-Affairs-and-International-Cooperation-15-52-39.

Law enforcement operations targeting money laundering networks in Viet Nam

There have been some raids targeting illegal online gambling and cyber-enabled fraud sites in Viet Nam, however, they have mostly been small in scale. While Viet Nam has managed to prevent large-scale establishment of physical operations in its territory, Vietnamese organized crime groups are active in the region, and its nationals make up a large portion of the regional cyber-enabled fraud workforce, consisting of both complicit individuals and others who are trafficked and forced into criminality. Within Viet Nam, law enforcement action has largely focused on targeting backend operations of gambling platforms, trafficking networks, and money laundering operations serving the regional industries, all of which have seen significant expansion in recent years.

For example, in August 2024, authorities in Viet Nam reported disrupting a local cell of a regional money laundering organization engaged in buying, selling, and illegally collecting local bank accounts and engaging in unauthorized peer-to-peer cryptocurrency services totalling more than 1.1 billion USDT in transactions between November 2023 to May 2024 alone.[31] The group was found to be systematically procuring hundreds of bank accounts and front company registrations from residents of Tây Ninh province for use by transnational criminal groups engaged in cyber-enabled fraud and money laundering operations in Cambodia.[32]

There are also indications of collusion between Vietnamese criminal actors and foreign counterparts. For example, one operation that was brought down in 2021 involved the laundering of funds from an online gambling website that had a turnover of almost US $3.8 billion. Investigations into the network remain ongoing, and police reported the 'mastermind' to be an Indian national.[33] More recently in 2024, Ho Chi Minh City police arrested members of a transnational crime group based in Viet Nam with links to Cambodia, including Vietnamese and Nigerian nationals.[34] The group was found to have been involved in more than US $78 million in transactions mostly from business email compromise fraud. To facilitate these transactions, members had established over 250 shell companies.

31 Ministry of Public Security of Viet Nam, Tay Ninh Provincial Police, Media Release, August 2024.

32 Ibid.

33 Ho Chi Minh City Police, "Ho Chi Minh City Police dismantled a large-scale gonline ambling ring and gambling organization", 2 December 2021, available at: https://congan.hochiminhcity.gov.vn/wps/portal/Home/trang-chu/noi-dung-chi-tiet/trang+chu/su+kien+noi+bat/catp+triet+pha+duong+day+danh+bac+quy+mo+lon+tren+mang.

34 Ho Chi Minh City Police, "Ho Chi Minh City Police dismantled an organized crime ring with foreign elements operating in 'Money Laundering' and 'Illegally transporting currency across the border'", 27 April 2024, available at: https://congan.hochiminhcity.gov.vn/wps/portal/Home/trang-chu/noi-dung-chi-tiet/anninhtrattu/tin+tuc+an+ninh+trat+tu/catphcm+triet+pha+duong+day+toi+pham+co+to+chuc+co+yeu+to+nuoc+ngoai+hoat+dong+rua+tien+van+chuyen+trai+phep+tien+qua+bien+gioi.

Geographic shifts, expansion, and establishment of new sites of operation

A key feature of Southeast Asia's evolving online crime industries is their mobility. As operators spread across the region, movement within countries and across the various porous borders has been extensive. In some cases, this movement has been prompted by external factors including law enforcement and conflict. For example, in 2019 when Cambodia announced a ban on online gambling, and in 2022 when it launched a series of raids focusing on Sihanoukville, large numbers of people left the coastal city, resulting in the temporary closure and abandonment of many operations temporarily ceased. Reports at the time indicated that these groups moved to other parts of the country or to Myanmar and Lao PDR , before their partial return.

Subsequent upticks in law enforcement operations in Lao PDR have led to significant migration of workers and criminal operations, with reports by law enforcement authorities and anti-trafficking organizations, as well as media monitoring, confirming large-scale movement back and forth between the GTSEZ and Tachileik in Myanmar, as well as Myanmar-based groups migrating to Cambodia through Lao PDR and Thailand. In addition to information gleaned from various online forums and Telegram channels, regional law enforcement agencies as well as anti-trafficking in persons and rescue groups have confirmed these shifts are taking place after gathering testimonies from survivors and migrating criminal groups in detention. Various reports on police actions in border areas have also revealed increased movement, with groups of mostly young males regularly apprehended crossing from Lao PDR to Cambodia, often lacking any travel documents.





Foreign nationals apprehended crossing the border from Lao PDR to Cambodia, August 2024. Source: Commissariat Police of Preah Vihear Province, Cambodia.

As detailed earlier, the conflict and crackdowns in the north of Myanmar led to both internal and cross-border migration of operations. Thai authorities have intercepted people suspected of moving between cyber-enabled crime operations in Myanmar en route to Cambodia, sometimes in possession of large amounts of equipment. Additionally, prior to Thailand cutting power to Myawaddy in February 2025, there was already some movement of operators to the south of Myawaddy, especially the area of Payathonzu, which is controlled by the Democratic Karen Buddhist Army (DKBA), as confirmed by regional law enforcement.[35] The DKBA and the Karen Border Guard Force recently repeated public calls for online scam operators to leave the areas they administer, and in the midst of Thailand's border crackdown have said they will continue to investigate suspicious sites, which could result in further migration. While some groups will inevitably relocate, others may wait to see if ongoing law enforcement action is sustained.

35 UNODC, "Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud", Bangkok, Thailand, August 2024; National Police Agency of Japan, "Global Fraud Meeting", Tokyo, Japan, September 2024.



Police seizure of call centre equipment being transported from Myanmar to Cambodia via Thailand, including 1,251 mobile phones, 274 SIM cards, and 19 sets of computer equipment, February 2025. Source: Pattaya Mail.

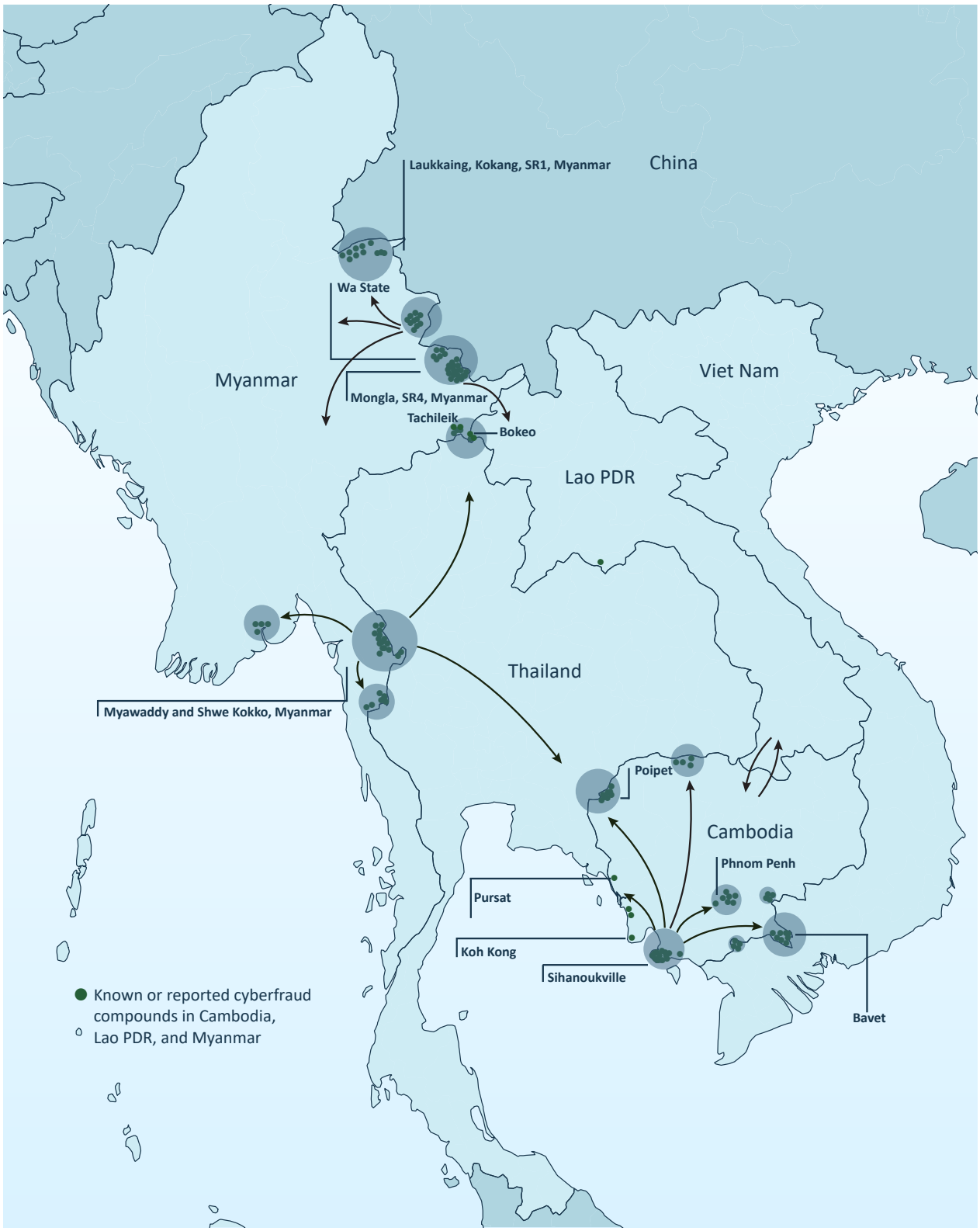
Recent developments in the Philippines have also shown some indication of cross-border movement. Online gambling and cyber-enabled fraud operators have sought to evade the POGO ban, but the PAOCC has already identified groups moving to find more secure locations to operate. In February, the PAOCC and local police forces rescued more than 30 Indonesian nationals from a Chinese-run online operation in Pasay. The company had halted its activities in January 2025 and was planning to relocate to Cambodia. When several workers refused to move, they were threatened and their supervisors demanded a fee to return their passports, leading to complaints by the captive Indonesians that precipitated the raid.[36]

In the midst of these shifts, with the industry embattled and moving out of certain areas, expansion can be observed in other areas that have not been subject to sustained law enforcement action, in some cases on a massive scale. As noted above, there have been periods of increased law enforcement activity in Cambodia that have targeted well-known epicentres of online gambling and cyber-enabled fraud. While this dampened the expansion of these industries in some more visible and accessible locations, it led to significant expansion in more remote locations.

In coastal and rural areas of Koh Kong, as well as areas bordering Thailand and Viet Nam, existing sites have expanded, and several entirely new hubs have been constructed in the last one to three years. In Myanmar, major crime sites have also expanded at a rapid pace in recent years, with indication of new sites also being developed, particularly south of Myawaddy, although official reporting remains limited.

36 Presidential Anti-Organized Crime Commission, "PAOCC and PNP Joint Operation in Pasay and Parañaque City Resulting in the Rescue of 31 Foreign Nationals", 13 February 2025.

Map 1. Locations of known or reported scam centres in the Mekong region 2023 - 2025



Online operations and workers move both within and across borders in the Mekong region. Source: UNODC.

Figure 1. Expansion of select sites hosting online gambling and cyber-enabled fraud operations 2021 - 2025[37]



Pursat, Cambodia, February 2022 to January 2025. Source: Google Earth.



Koh Kong, Cambodia, December 2023 to December 2024. Source: Google Earth.



Tbong Khmum, Cambodia, December 2023 to January 2025. Source: Google Earth.



KK Park, Myawaddy, Myanmar, April 2022 to December 2024. Source: Google Earth.

37 Locations identified or confirmed by reigonal law enforcement agencies and anti-trafficking in persons organizations based in Southeast Asia, 2025.



Yatai New City, Shwe Kokko, Myanmar, March 2022 to December 2024. Source: Google Earth.

These trends of mobility and entrenchment exist in parallel. While law enforcement activity both within countries and by neighbouring countries and other external actors is having an impact, the continued emergence and expansion both at scale and at a rapid pace suggests there is a level of comfort within the industry that it can endure the various pressures it currently faces. At the same time, reports continue of East and Southeast Asian organized crime groups expanding their activities globally. This potentially reflects both a natural expansion as the industry grows and seeks new bases and marketplaces, as well as a likely hedging against future risks should disruption continue and intensify in the Southeast Asia region.

Operational adaptation

Additional to geographical pivots, regional crime groups have proved capable of rapidly adapting their operations to changing circumstances. As demonstrated by the ban on POGOs in the Philippines, while operations were disrupted, law enforcement in the region continues to raise concerns of criminal groups finding new covers for their activities.

Following the enactment of the ban, there was an increase in law enforcement activity. Large numbers of arrests have been made and hundreds of workers deported to their home countries. However, soon after the ban was announced, authorities expressed concerns over how entrenched illegal offshore gaming operators have become, with hundreds of POGOs continuing to operate despite having their licenses cancelled even before the ban came into force.[38] This was underscored by the Philippine Amusement and Gaming Corporation (PAGCOR), which revealed in June 2024 that 250 to 300 offshore gambling firms were operating illegally in the Philippines without licenses.[39]

Since the ban, the PAOCC has said former POGOs have rebranded as business processing outsourcing operations (BPOs) or moved into the premises of other BPOs. The BPO industry in the Philippines employs many thousands of people and involves taking contracts from global companies to provide services such as call centres, IT back-end support, software design, and animation, among others. BPOs may be located in office towers and business parks, and as such provide useful cover for illegal online operations.

In addition to those operating under the cover of BPOs, in November 2024, PAOCC's director referred to 'guerilla POGOs' that have broken up into smaller cells and scattered themselves in residential areas, casinos, resorts, and special economic zones.[40] An investigation by the Senate Committee on Women, Children, Family Relations, and Gender Equality reached similar conclusions, and when presenting the report, Senator Risa Hontiveros stated: "These criminal networks are highly adaptable, and they are already using new cover operations to continue their illicit activities … POGOs may be gone in name, but the damage they caused—and their ability to morph into other businesses—remains a national threat."[41]

38 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

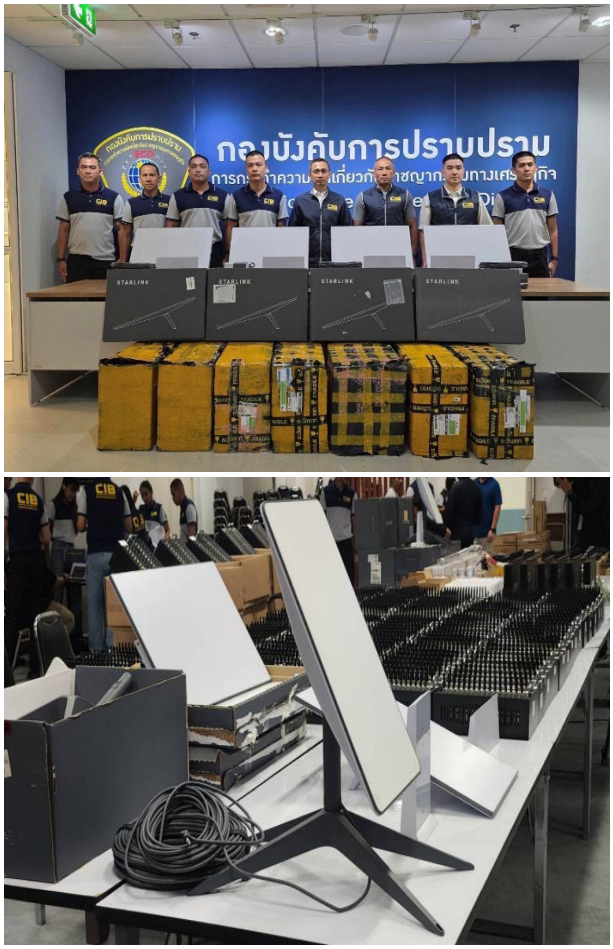
39 Reuters, "PAGCOR Chairman Alejandro Tengco in interview with Reuters", June 2024, available at: https://www.reuters.com/world/asia-pacific/philippines-cracks-down-illegal-offshore-gambling-firms-2024-06-13/.

40 PAOCC, "Director Winnie Quidato speaking at the Senate Committee on Women, Children, Family Relations and Gender Equality", November 2024.

41 Philippines Senate Committee on Women, Children, Family Relations, and Gender Equality, "Committee Report No. 514", 3 February 2025, available at: https://web.senate.gov.ph/lisdata/4587041906!.pdf.



Joint law enforcement operation raids fraudulent online gaming operation in Pasay, arresting six Koreans and 15 Filipinos, February 2025. Source: PAOCC, February 2025.



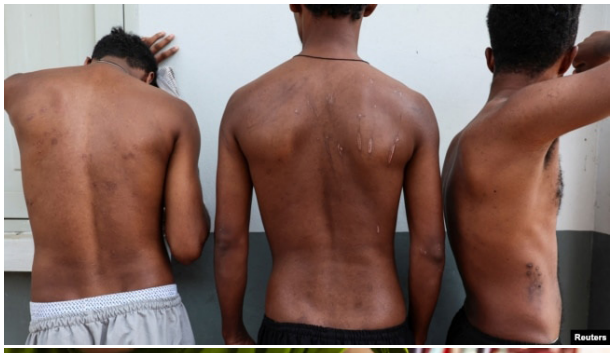
58 Starlink devices seized by Thai authorities that were ready to be shipped to the Myanmar and Cambodian borders, June 2024. Source: Bangkok Post / Starlink devices, SIM boxes and over thirty thousand Thai and Hong Kong SIM cards seized in Chiang Mai, May 2024. Source: Thai PBS.

Another adaptation that has been noted across the region is the shift from land-based internet connection to Starlink. In some cases, this has been necessary as operators move to remote locations without access to internet infrastructure. In others, the shift has been brought about due to cross-border internet wires being severed and communication towers being dismantled. In areas of Cambodia and Myanmar bordering Thailand, online gambling and cyber-enabled fraud operations have routinely utilized illegal cross-border connections. As pressure has grown in Thailand to crack down on the industry, many of these connections have been dismantled, causing the industries to adapt. Recent drone imagery of several major scam compounds in Myawaddy, for instance, has shown dozens of Starlink receivers mounted onto the roofs of various buildings, with regional law enforcement reporting regular seizures at raided sites or interceptions as they are transported between countries where Starlink is illegal.

Digital infrastructure has also developed and evolved rapidly as operators pivot to create their own ecosystems consisting of online payment applications, encrypted messaging platforms, and cryptocurrencies and exchanges, to circumvent mainstream platforms that are coming under increasing pressure to take action against actors using their services for illicit activities. Another crucial shift has been the rapid diversification of the online workforce. Once dominated by people from mainland China and other Sinophone countries and regions, there are now dozens of nationalities recorded in online compounds. This pivot reflects, in part, an evolution of the industry, as it expands and seeks out new potential markets. However, it also likely indicates operators hedging against the risk of law enforcement action in target markets restricting operations and creating challenges in recruiting workers, as has been the case with China, which has increased scrutiny of outbound travelers to online hotspots.

Trafficking in persons for forced criminality - diversification of nationals

As has been documented at length elsewhere, regional cyber-enabled fraud and other online crime operations are deeply implicated in trafficking in persons for forced criminality.[42] There has been extensive reporting on cases of people being tricked into online compounds with fake job offers, forced to work, and sold between operators. Even those who enter the industry willingly may find themselves trapped, locked in debt to scam operators, with their passports and other documents held by operation management. Violence within the industry is commonplace, with physical punishment commonly meted out on those who fail to comply or hit performance targets.





Top: Ethiopian citizens released from scam compounds in Myawaddy in February 2025 show injuries from beatings and electric shocks. Source: Reuters. Bottom: Victim released from Myawaddy in February shows journalists his injuries. Source: Reuters, 2025. AFP, 2025.

While the bulk of the online gambling and scam industry workforce was initially made up of mainland Chinese nationals, it has diversified rapidly in recent years. This reflects the industries' expansion into new markets. Online gambling platforms have large cohorts of agents who work to attract people to their platforms, as well as customer service operators, so a workforce that can speak the language of the target market is important. Scam operations are increasingly utilizing new technologies and artificial intelligence to target victims globally. This includes large language models for translation and deepfake filters for video calls and other fraudulent online content and advertisements. However, having workers who can speak the language of their target, and know the social and cultural quirks that will make their pitches more convincing, significantly increases the chance of success.

It is difficult to estimate with certainty the numbers of people working, either willingly or unwillingly, in the regional cyber-enabled fraud industry. Nationals from more than 50 countries have been identified, as evidenced by information gathered from reports by police, anti-trafficking groups, industry chat groups, as well as statements from embassies, and interviews with groups engaging directly with survivors of the compounds. Chinese nationals still make up a large segment of foreign workers in regional cybercrime sites, alongside Vietnamese, Indonesian, Malaysian and Thai nationals.[43] Myanmar, Philippine and Lao nationals are present in significant numbers in compounds in their home countries, but are also present elsewhere in the region.[44] Geographical proximity and relaxed travel restrictions within ASEAN makes travel for these people logistically more straightforward without the same checks and balances in place as for other non-ASEAN citizens and less expensive. Additionally, Thailand, Viet Nam, and Indonesia – where gambling is is largely prohibited for locals – represent massive markets for illegal online gambling, making workers from these countries especially sought after.

As noted earlier, in February this year, following high-level dialogue between China, Thailand and Myanmar, cross-border power transmission from Thailand to Myanmar was cut, along with export of fuel supplies. Myanmar non-state armed groups controlling areas along the border where online crime sites have flourished inspected several sites and removed thousands of people. In February, three major handovers occurred, with around

42 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, p.43-48; International Organization for Migration, "IOM's Regional Situation Report on Trafficking in Persons into Forced Criminality in Online Scamming Centres in Southeast Asia", February 2024; UNODC, "Policy Brief: Casinos, cyber fraud and trafficking in persons for forced criminality in Southeast Asia", August 2023; UNOHCHR, "Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response", August 2023.

43 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

44 Although precise figures are not available, this conclusion is drawn from an assessment of reporting over the past four years and discussion with groups supporting victims.





Indian nationals released from Myawaddy scam compounds are repatriated by Indian military from Thailand, March 2025. Source: Indian Embassy in Thailand.

800 people handed to Thai border authorities for processing. The make up of these groups provides a useful illustration of how diverse the online workforce has become.

Two large groups were handed over in February by the Karen Democratic Buddhist Army and the Karen Border Guard Force, respectively. Within these groups, 23 nationalities were represented.[45] A third group consisted of over 200 Chinese nationals, who were handed over at the border and swiftly placed on chartered flights back to China.[46] In late February, 2025, the Karen Border Guard Force stated that it was holding over 7,100 people who had been removed from online compounds.[47] More than half were Chinese, with the remainder made up of over 27 other nationalities.

Several more repatriations of Chinese nationals occurred via Thailand, with the total number reaching 2,876 by mid-March.[48] Statements from the Chinese Government described them as fraud suspects and images showed people disembarking planes in China in handcuffs. The Indian Government also mobilized to repatriate citizens that were handed over by Myanmar authorities on the Thai border, with military planes sent to pick up more than 550 people. In contrast, they were described by the Indian Embassy as being 'rescued' after being "lured with fake job offers and were made to work in scam-centers".[49]

The situation on the Thai-Myanmar border is complex, but lays bare a humanitarian crisis that has been building for at least five years. As the online crime industries have expanded, the workforce has grown rapidly, drawing in people from across the world, many trafficked and working under conditions of extreme cruelty, bonded to their 'employers' often with little chance of being rescued by authorities.

Those who arrived in Mae Sot, Thailand, in February spoke of appalling conditions in the compounds in Myanmar, and many showed old scars and fresh wounds inflicted by those holding them. Across the region, victim identification is often a slow process, and in many instances, existing regulatory frameworks are not well suited to appropriately assess victims of forced criminality. Thai authorities faced the prospect of processing thousands of people, many without any form of documentation. Several countries whose nationals were released do not have embassies in Thailand, further complicating the situation. By the end of March, according to the Myanmar military, 8,709 people had been identified and detained in Myanmar, with 6,307 already deported to Thailand.[50]

Both the Karen Border Guard Force and the Democratic Karen Buddhist Army have said the cost of housing the thousands of people that have been removed from the compounds is a massive burden. Many survivors have physical and mental health issues, and need to be fed, clothed and provided with shelter until Thailand is able to accept them and process them for repatriation.

There remain many tens of thousands of people working in online operations in Myanmar and across the region. Committed effort is needed

45 Royal Thai Police, "Stakeholder Roundtable Closed- Door Meeting", Bangkok, Thailand, February 2024.

46 Chinese Embassy in Myanmar, "The first batch of 200 Chinese fraud suspects in Myanmar's Myawaddy region were escorted back to China via Thailand", 20 February 2025, available at: https://mp.weixin.qq.com/s/RfgQf5WjEdwpdLD4CXDNCQ

47 According to data shared by the Karen Border Guard Force with local Thai media, 'The Reporter', February 2025.

48 Criminal Investigation Bureau of the Ministry of Public Security of the PR China, "A total of 2,876 Chinese fraud suspects in Myanmar's Myawaddy region were escorted back to China in batches via Thailand", 14 March 2025, available at: https://mp.weixin.qq.com/s/TtCiR3pl-aU6vEAh9UXpRw

49 Indian Embassy in Thailand, "Secured repatriation of 549 Indians through Mae Sot in Thailand to India on 10 and 11 March 2025 by two special flights", 12 March 2025, available at: https://embassyofindiabangkok.gov.in/.

50 Myanmar News Agency, "144 Chinese nationals deported, 39 more detained for telecom fraud, Global New Light of Myanmar", 29 March 2025, available at: https://www.gnlm.com.mm/144-chinese-nationals-deported-39-more-detained-for-telecom-fraud/.

Table 1. Breakdown of workers removed from Myawaddy compounds in February, 2025.

Handed to Thai authorities 12 Feb		Handed to Thai authorities 27 Feb		Awaiting repatriation in Myanmar as of 26 February			
Nationality	# of people	Nationality	# of people	Nationality	# of people	Nationality	# of people
Ethiopia	138	Ethiopia	192	China	4,860	Nigeria	7
Kenya	24	Kenya	31	Viet Nam	572	Ghana	6
Philippines	16	Indonesia	13	India	526	Cameroon	6
Malaysia	15	Lao PDR	13	Ethiopia	430	Bangladesh	6
Pakistan	12	Uganda	12	Indonesia	283	Namibia	4
China	10	Sri Lanka	13	Philippines	127	Rwanda	4
Indonesia	8	Pakistan	9	Malaysia	69	Tunisia	3
Nepal	7	Philippines	8	Pakistan	68	Czechia	2
Lao PDR	6	Liberia	5	Kenya	64	Lao PDR	1
Uganda	6	Nepal	4	Nepal	17	Romania	1
Bangladesh	2	Sierra Leone	4	South Africa	17	Algeria	1
Brazil	2	Ghana	3	Sri Lanka	8	Singapore	1
Burundi	2	Nigeria	3	Uzbekistan	8	Others	34
Cambodia	1	Burundi	2				
Ghana	1	Rwanda	2	**Total**		**7,141 (425 female)**	
India	1	Cameroon	1				
Nigeria	1	India	1				
Sri Lanka	1	Malaysia	1				
Other	7						
Total	**260 (37 female)**		**317 (55 female)**	*Note: A third group of around 200 Chinese nationals was handed to Thailand and repatriated in February, 2025.*			

Source: Royal Thai Police, Karen Border Guard Force, and Chinese Embassy in Myanmar, 2025.



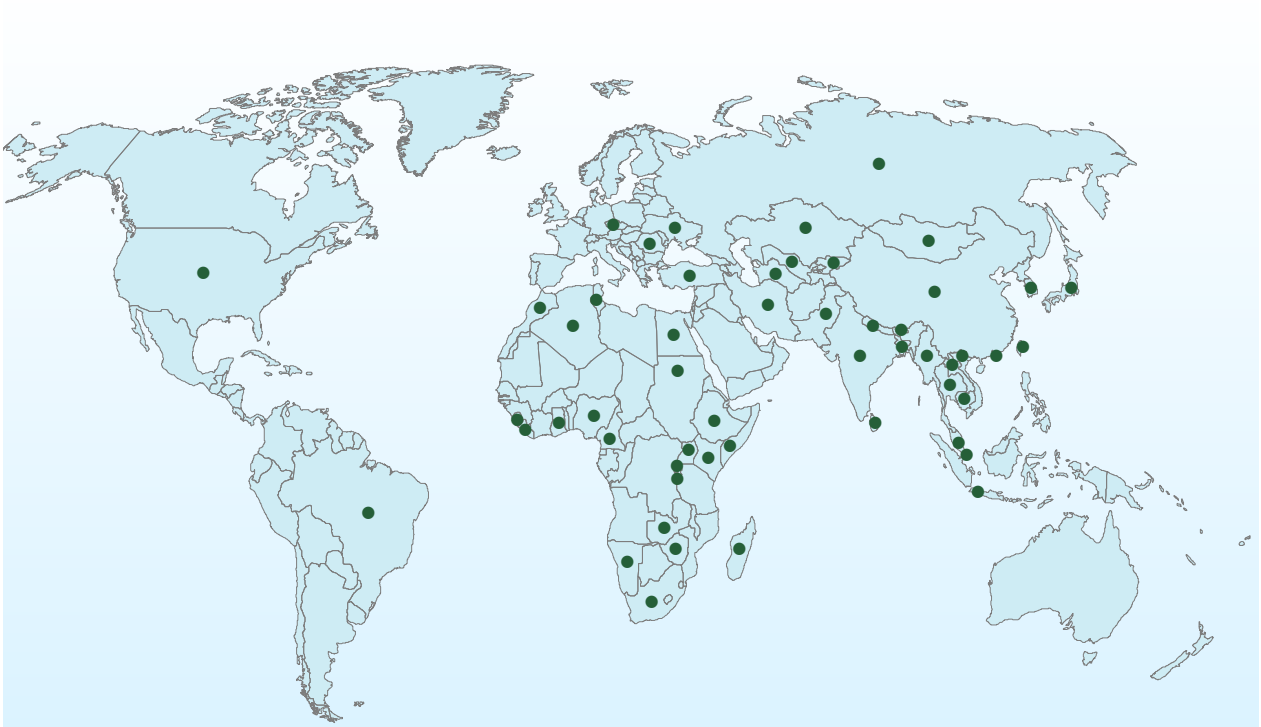
Source: Myanmar National Portal, February 2025.

to eliminate these operations, and as illustrated in Myawaddy, this needs to be matched by preparations to provide humanitarian assistance and ensure that processes are in place to rapidly assess and repatriate those released or rescued. The longer the industry is allowed to continue to grow and operate, the bigger the humanitarian crisis will be if and when major counter actions occur.

Scam operations remain active elsewhere in Myanmar, including in the north. Law enforcement action and conflict resulted in many operations closing and saw thousands deported, but many simply relocated to more remote areas. In some locations the conditions are extremely rudimentary, as evidenced in images released by the military after raids in Shan State in February on a site housing Chinese, Vietnamese, and Myanmar citizens.

Beyond Myanmar, the situation across the region remains dire. Embassies and other state institutions from China, India, Sri Lanka, Nepal, Pakistan, the Philippines and many others, have issued warnings to their citizens about the risks associated with travel to Cambodia, Lao PDR, Myanmar, and Thailand.

Map 2. Origins of people identified in regional scam compounds



Africa	**East Asia**	**Central Asia**
1. Algeria	23. China	43. Kazakhstan
2. Burundi	24. Hong Kong SAR	44. Kyrgyzstan
3. Cameroon	25. Japan	45. Turkmenistan
4. Egypt	26. Mongolia	46. Uzbekistan
5. Ethiopia	27. Republic of Korea	**West Asia**
6. Ghana	28. Taiwan PoC	47. Iran
7. Kenya	**Southeast Asia**	**Asia/Europe**
8. Liberia	29. Cambodia	48. Georgia
9. Madagascar	30. Indonesia	49. Russia
10. Morocco	31. Lao PDR	50. Türkiye
11. Mozambique	32. Malaysia	**Europe / North America**
12. Namibia	33. Myanmar	51. Czechia
13. Nigeria	34. Singapore	52. Romania
14. Rwanda	35. Thailand	53. Ukraine
15. Sierra Leone	36. Viet Nam	54. United States
16. Somalia	**South Asia**	**South America**
17. South Africa	37. Bangladesh	55. Brazil
18. Sudan	38. Bhutan	56. Colombia
19. Tunisia	39. India	
20. Uganda	40. Nepal	
21. Zambia	41. Pakistan	
22. Zimbabwe	42. Sri Lanka	

Source: UNODC review of official reports, statement from embassies and foreign affairs ministries, information provided by anti-trafficking in persons organizations. Note: There are likely to be more nationalities that authorities are not yet aware of.

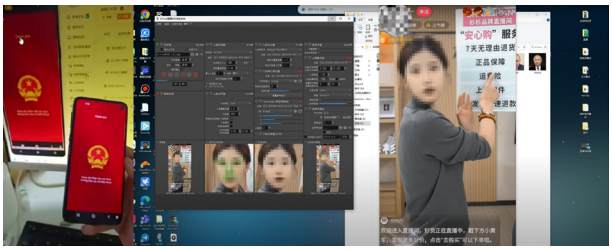
Impact of industry professionalization, innovation, and evolution

While trafficking for forced criminality connected to scam centres persists at high levels throughout Southeast Asia, there is strong indication of a shifting business model and growing professionalization within the regional cyber-enabled fraud industry. Much of this has been driven by the emergence of new illicit online marketplaces, particularly those based on Telegram, that are native to Southeast Asia and have fundamentally revolutionized the way in which transnational criminal networks operate. This development has fueled rapid industry expansion as well as other areas within the illicit economy, and exacerbated existing challenges to contain the situation.

Telegram's ease of access, mobile-first design, strong encryption, real-time messaging, and automation via bots has made it more convenient and scalable for illicit actors in Southeast Asia compared to the dark web, which requires knowledge, lacks real-time interactions, and has greater technical barriers. Several Telegram-based platforms controlled by some of the region's most powerful and influential regional criminal networks have emerged in recent years, representing key venues where criminals and service providers from various parts of the region may congregate, connect, and conduct business online. These marketplaces, which are often connected to parallel cryptocurrency exchanges controlled by the same entity, host a wide range of merchants specializing in the sale of stolen data, hacking tools, malware, and various underground banking, money laundering and cybercrime services utilized by other criminals, and particularly those engaged in cyber-enabled fraud.

The rise of large peer-to-peer marketplaces and the corresponding influx of illicit service providers has been consistent with latest trends reported by regional law enforcement and cybercrime investigators. This has been particularly noticeable in relation to deepfakes, sextortion, and malware-enabled fraud incidents which have increased dramatically across East and Southeast Asia in recent years, with growing attribution being made to local criminal networks and scam centres.[51]

The professionalization of associated recruitment agencies servicing the scam industry on these marketplaces has also continued to attract thousands of underemployed and disenfranchised youth from many of the world's poorer countries to seek and pursue opportunities within it despite the high levels of risk and deception involved.



Screen capture of demos shared by malware and deepfake software vendors advertising solutions to Mekong-based criminal groups engaged in police impersonation fraud identified by ChongLuaDao (Viet Nam) and UNODC researchers, 2024.

In addition to managing these large online marketplaces, many of the entities behind them possess well-documented and direct ties to organized crime groups, with a growing number amassing enough wealth and influence to expand their business lines into the financial sector of targeted jurisdictions in the region. This has been most apparent in the case of illegal online gambling platforms, unauthorized payment processors, and virtual asset service providers which have proliferated throughout Southeast Asia and have begun expanding services globally. These entities often present themselves as legitimate and registered financial businesses, despite being wholly unauthorized to engage in online betting, payment processing and cryptocurrency-related activities, operating with virtually no regulatory overhead as they service criminal industries.

The development of these digital solutions for money laundering and underground banking has overwhelmed local and international authorities and enabled the sustained expansion of the criminal business environment across Southeast Asia, effectively securing high-speed channels for integrating billions in criminal proceeds into the formal financial system with impunity. This has in turn attracted new criminal networks, innovators, and specialist service providers to enter illicit markets while simultaneously driving demand for new underground banking channels connecting Southeast Asia and other regions to be created.

51 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*.

Evolving tradecraft of transnational organized crime in Southeast Asia: Unmasking the Vault Viper network

Asian crime syndicates are highly entrepreneurial and known to mask their criminal operations and illicit financial flows as legitimate business interests and investments. While many sectors are targeted by these powerful networks, this has been most apparent in the case of capital-intensive businesses including integrated casino resorts, hotels, junkets, and severely underregulated online gambling and digital payment platforms around which Asian organized crime has converged.[52,53]

Gambling and related businesses have been widely designated as high risk in many parts of the Asia Pacific region, commonly found to be misused by organized crime to expand influence, conceal illicit activities, and transfer value across borders undetected.[54,55] Criminal groups engaged in these complex, interconnected industries have built out their portfolios in jurisdictions deeply challenged by weak or virtually nonexistent regulatory frameworks and low levels of investor screening, threat awareness, and enforcement capabilities. In certain cases, they have also co-opted local officials as key partners and enablers through corruption and various political contributions and lobbying, with 'investments' into such industries providing unprecedented operational utility, influence, and access to illicit actors.

In recent years, these networks have aggressively diversified their business lines by pivoting off unregulated and often illegal online gambling operations into various financial and cybercrimes, exploiting gaps in the regulation and monitoring of highly technical supply chains, transactions, and money flows involved in online betting. This has necessitated the continued evolution of their tradecraft, and has culminated in a complex criminal ecosystem involving intricate layers of technical, financial, legal, and regulatory obfuscation and related service providers used to impair investigators and overwhelm government systems while enabling further expansion.

Building on past UNODC analyses, in 2024 UNODC and collaborating security experts identified a cluster of illegal online gambling websites involved in malware distribution owned and operated by criminal groups known by regional law enforcement agencies to be engaged in large-scale cyber-enabled fraud, trafficking in persons, and money laundering operations. As is often the case with unlicensed, illegal operators, comprehensive analysis of the cluster's domain name system (DNS)[56] infrastructure reveals a direct relationship with a leading iGaming software provider to which they all redirect.

Known within the industry as white-label platforms, these large business-to-business service providers offer turnkey solutions allowing customers to launch fully functional gambling websites with minimal technical involvement. White labels typically integrate a suite of services including various casino games and sportsbooks, backend management tools for user data, affiliate systems, analytics, fraud monitoring, customer support integration, and optional know your customer (KYC) and anti-money laundering (AML) compliance modules. The software is highly customizable, allowing for localization in language, payment options, and promotions to target specific markets where online betting is strictly regulated or prohibited.

DNS infrastructure is critical for illegal online gambling operators in maintaining user access and resilience against enforcement actions, however, mapping these networks through DNS can be challenging. Illegal operators use elaborate web architecture consisting of large numbers of randomly generated domain names to spread their infrastructure and hedge against disruptions caused by domain blocking or takedowns. Providers and operators often register large numbers of these domains through offshore or privacy-protecting registrars, utilizing

52 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in southeast Asia: A Shifting Threat Landscape*.

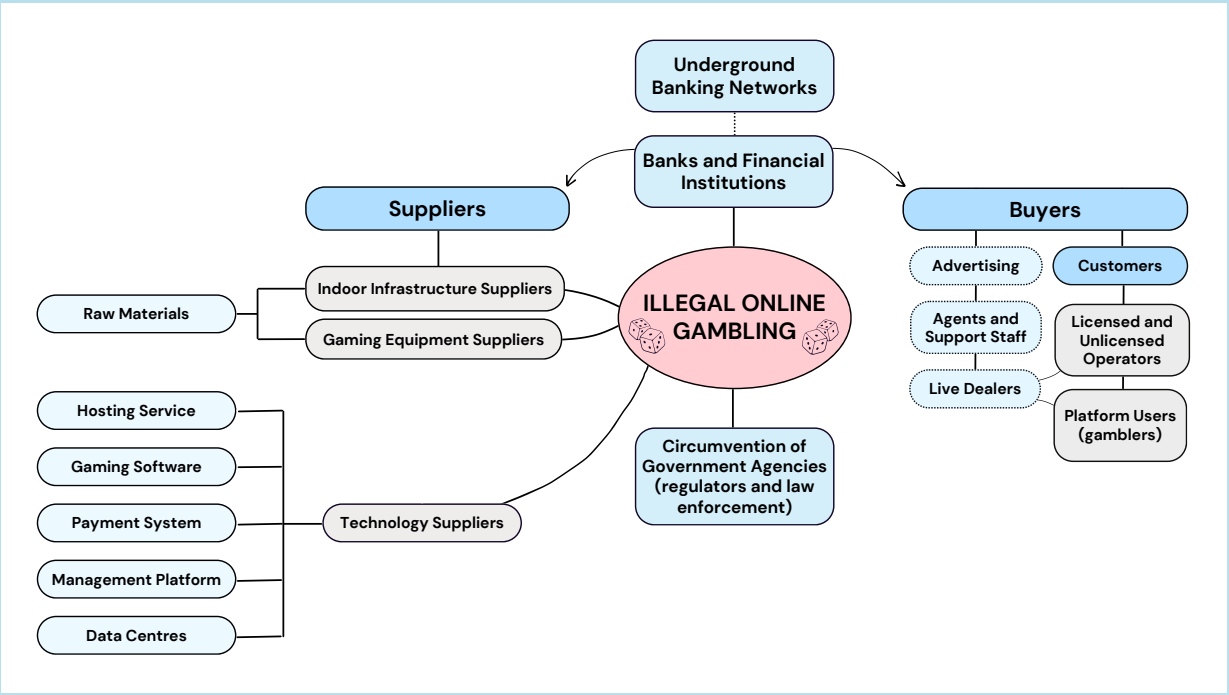
53 UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*.

54 UNODC, "Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact", October 2024.

55 UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*.

56 DNS is a protocol that translates domain names into numerical IP addresses, enabling computers to locate and communicate with each other over the internet.

Figure 2. Simplified illegal online gambling supply chain



Elaboration based on consultations with enforcement authorities, security researchers, and industry experts. Source: UNODC, 2025.

DNS management services that allow for rapid domain changes and redirection in such cases. Those operating in black (illegal) markets also employ Content Delivery Networks (CDNs) and DDoS protection services to ensure uptime and mitigate traffic monitoring by authorities, while domain fronting[57] is commonly used to obscure the actual server endpoints.[58] They also integrate with third-party payment gateways, using unlicensed alternative or crypto-based solutions to avoid banking restrictions and ensure funds flow seamlessly in and out of high-risk regions. Despite these various configurations and tactics, the abovementioned service provider and de facto malware distributor, named Vault Viper by security researchers and known formally as Business Group 1 (BG 1), features a distinct DNS fingerprint, making it possible to accurately interpret, trace, and analyze.

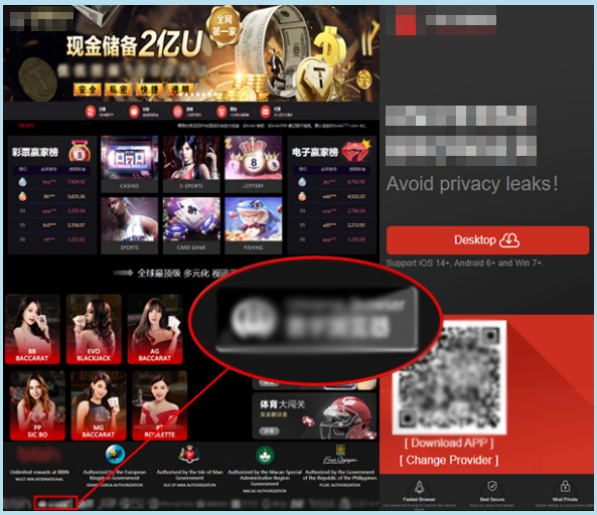
Founded in Taiwan PoC more than two decades ago, BG 1 is made up of a vast, global network of subsidiaries, shells, and offshore holdings. It has established several hotels and casinos as well as large-scale technology and data operations in Southeast Asia as a leading iGaming service provider, enabling its online gambling platform to emerge as one of the largest and most successful turnkey iGaming solutions in Asia. The platform offers a fully customizable white label solution covering everything from platform development and game integration to backend management, security, and payment processing.

BG 1 has maintained a large operational base in the Philippines since 2006, particularly in the Clark Freeport and Special Economic Zone, through its subsidiary, Technology Company 1 (TC 1), and parent company, Parent Company 1 (PC 1), which also oversees a large hotel and licensed casino resort, among other projects. The full extent of the Group's operations and ownership structure, however, are largely concealed through a tangled web of companies registered in countries and territories including Belize, the British Virgin Islands, China (including Hong Kong, Macau, and Taiwan PoC), Malta, and Samoa, with BG 1-supported online gambling websites regularly displaying iGaming authorizations from regulators in the Isle of Man, Macau, Malta, and the Philippines, including PAGCOR and the Cagayan Economic Zone Authority (CEZA).

57 Domain fronting is a technique used to disguise the true destination of internet traffic by routing it through a legitimate, high-reputation domain (often belonging to major cloud service providers like Google, Amazon, or Cloudflare). It is commonly used to bypass censorship, firewalls, or evade surveillance, but may also be exploited for malicious purposes.

58 A server endpoint is the specific location on a network where a service or system receives and processes requests. It functions as a defined access point, allowing applications, platforms, or users to connect to a particular service, such as a database, website, or cloud-based tool. In the context of illicit online activity, for instance, a malware operator may configure a server endpoint to receive stolen data or issue commands to infected devices, making these endpoints critical targets for detection, disruption, and attribution efforts.

Adding to these concerns, the Group appears to have recently expanded operations into malware distribution through its integration of a malicious web browser, leveraging its status as a trusted iGaming solution to push the software to unsuspecting users.



Malicious web browser distribution through BG 1's white-label. Source: UNODC and Infoblox Researchers, 2025.

BG 1's white-label offers a two-click download to its recommended U Browser across all serviced websites. The modified Chrome-based browser purports to have been specifically developed for BG 1, created to enhance security, privacy, accessibility, and user experience for the iGaming platform's users. It is designed to bypass regional restrictions and internet censorship, which is particularly vital for operators targeting black markets including China where online gambling is illegal and access to such platforms is widely restricted and prohibited. The download is accessible across all BG 1-based online gambling websites as well as major mobile app stores, supporting Chinese, English, Korean, and Vietnamese languages.

As validated by Infoblox's Threat Intel Group, when the U Browser installer is run for the first time, it immediately checks for user location, language, and indicators signaling the presence of a virtual machine – a common technique used by malware to obstruct analysis. Once all checks are passed, the browser will wait for some time before connecting to specific attacker-controlled IP addresses in China and elsewhere in Asia. Upon successful installation, the user is presented with a modified variant of Chromium[59] which purports to offer a 'secure tunnel' service between the user and a VPN server to ensure protected user data and privacy. Unknown to the user, however, the browser's installer proceeds to introduce a number of persistent programs that run silently in the background.

While technical analysis is ongoing, preliminary examination reveals that U Browser not only enables involuntary, systematic screenshots to be taken on the infected device but also contains other hidden functionality allowing the software to capture keystrokes and clipboard contents – features consistent with malware evoking remote access trojans and various cryptocurrency and infostealers. Following installation, after some time the persistent binaries[60] will reach out to several different China-based IPs associated with command-and-control (C2) servers signed[61] by BG 1.

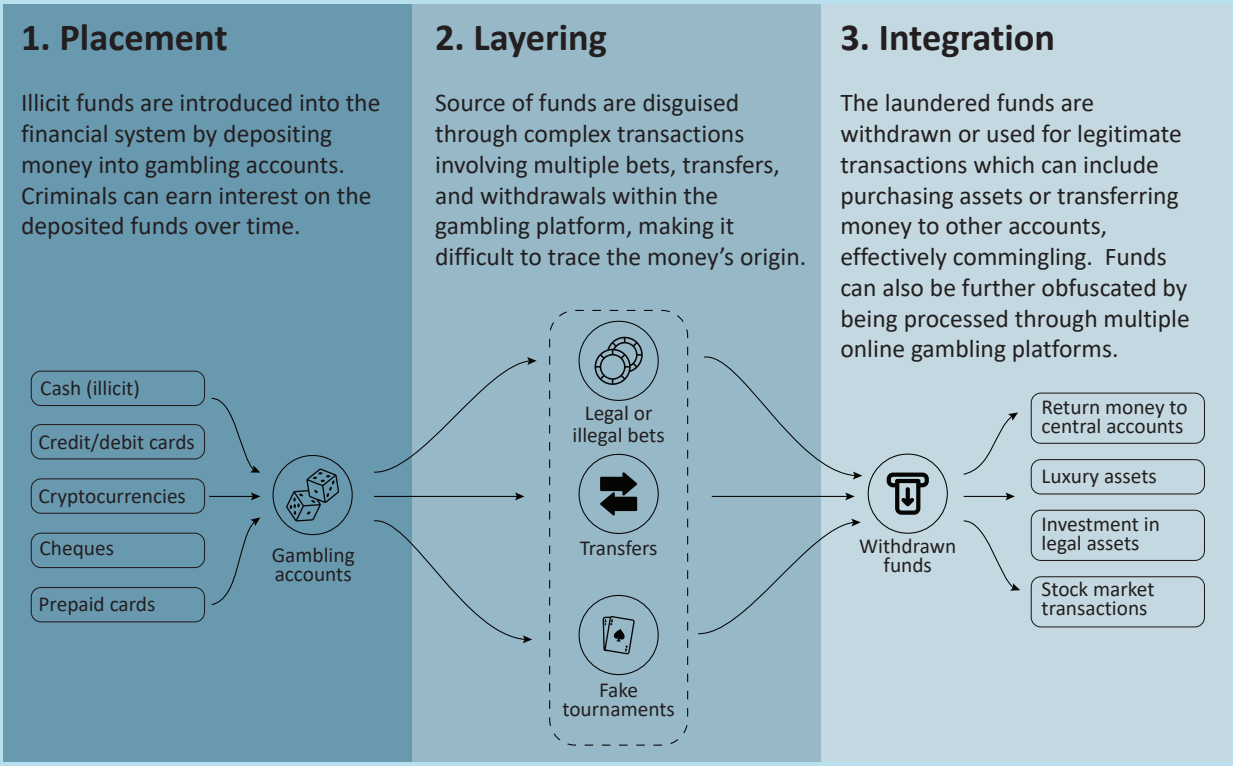
By analyzing the malware and mapping out the DNS infrastructure, Infoblox researchers were able to identify over 1,000 unique nameservers hosting thousands of active websites, with all dedicated to illegal online gambling, including several known to be operated by criminal groups involved in cyber-enabled fraud, trafficking in persons, and other illicit activities. This is consistent with prior reporting by regional law enforcement which has repeatedly implicated BG 1 in servicing illegal operators across East and Southeast Asia, including those engaged in online fraud and money laundering. This includes direct connections to major Taiwan PoC-based Triad groups including Bamboo Union, Four Seas Gang, Tian Dao League or Sun

59 Chromium is an open-source web browser project, primarily developed and maintained by Google, that serves as the foundation for many popular browsers, including Google Chrome and Microsoft Edge.

60 In the context of malware, a persistent binary refers to a malicious program or file that is designed to remain active on an infected system over an extended period of time, even after a reboot or system cleanup. It is specifically created to ensure the attacker maintains access to the system, often by running automatically upon startup or by re-infecting the system if it's removed.

61 Examination of Universe Browser's corresponding command-and-control (C2) servers reveals that the digital certificate associated with these servers' infrastructure is registered under BBIN. This is significant because digital signatures are normally used to verify the legitimacy and trustworthiness of software or online services. This adds a layer of legitimacy that can help the C2 servers evade detection, as they appear to be associated with a large, trusted entity. In the present context, this could point to either a supply chain compromise or potential complicity on the part of the service provider.

Figure 3. Utility of illegal betting for large-scale money laundering and underground banking



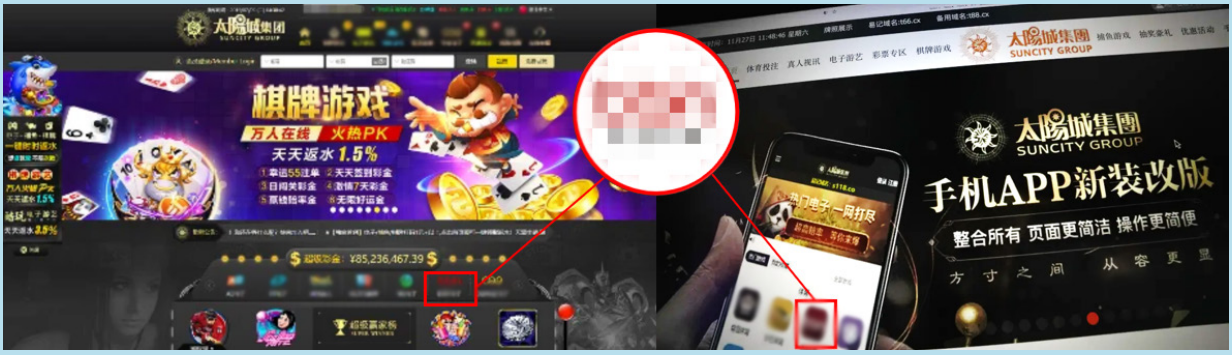
Source: Elaboration based on UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia (January 2024).

Alliance, and others operating in Cambodia, mainland China, Lao PDR, Malaysia, and the Philippines. In three major cases alone taking place between 2017 and 2023, the platform was found to have facilitated more than US $770 million in illegal online betting transactions for hundreds of thousands of users.[62,63,64]

Notably, further analysis of available corporate and DNS records, legal filings, and criminal case documents reveals substantial linkages between BG 1 and a major Hong Kong and Macau, China-based syndicate led by Suncity Group founder and convicted crime boss, Alvin Chau. As highlighted by prosecutors during his final sentencing hearing, as of January 2023, Chau was found to have held a majority of BG 1 shares, with his stake in the company, among many others, being used to increase the operating capital of parallel illegal betting and underground banking operations and decentralize risk across platforms.[65] More than this, authorities concluded that Suncity, at the time the world's biggest junket operator responsible for as much as 50 per cent of high-roller gambling turnover in Macau, China,[66] and proxy operations including BG 1, were utilized by Chau as a sophisticated front utilized by organized crime[67] – with investigations elsewhere further revealing Suncity's involvement in large-scale money laundering outside of China.[68,69]

Alvin Chau was convicted in China in January 2023 and sentenced to 18 years in prison on over 100 charges relating to facilitating illegal bets exceeding HK $823.7 billion (US $105 billion) between March 2013 and March 2021 through

62 Jiuquan City, Suzhou District Court, Press Release, March 2023.
63 People's Court of Yongding District, Zhangjiajie City, Hunan Province, Press Release, November 2017.
64 Taiwan PoC Police Agency, Central Investigation Bureau, Press Release, June 2024.
65 Acusação do Ministério Público, n.º: 1345/2022.
66 Hong Kong Jockey Club, Asian Racing Federation, 2023.
67 Acusação do Ministério Público, n.º: 1345/2022.
68 Parliament of New South Wales, Australia. "Casino Inquiry". 2021, available at: https://www.parliament.nsw.gov.au/tp/files/79129/Volume%201%20-%20Inquiry%20under%20section%20143%20of%20the%20Casino%20Control%20Act%20 1992.pdf.
69 UNODC, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat.



BG 1 iGaming infrastructure embedded within former Suncity Group online betting platform, 2019 - 2021. Source: Suncity Group (2019) and Associated Press (2021).

multiplier betting,[70] utilizing Suncity corporate, financial, and technological infrastructure, resources, and partnerships to conceal related transactions.[71] Digital evidence and other data recovered and reported by Chinese authorities notably indicate that at least 300 billion yuan (US $42 billion) in illegal bets were processed through the Group's offshore online betting operations between 2015 – 2019 alone.[72]

In addition to Alvin Chau, the Wenzhou Intermediate People's Court convicted 36 individuals affiliated with the syndicate, finding that the group provided cross-border currency exchange and settlement services and collected gambling debts through asset management companies and underground banks it had established in mainland China.[73] The Court determined that between 2016 and 2021, the Suncity-linked network had expanded to more than 280 mainland Chinese shareholder-level agents who capitalized the shadow business, as well as more than 38,000 multi-level gambling agents and promoters, and 80,000 clients (players).

Separately, in February 2024, authorities in Hubei sentenced 13 senior members of a Philippine-based illegal offshore gambling network specifically using Suncity and BG 1 infrastructure to recruit and service more than 250,000 gamblers across 25 Chinese provinces, with the network facilitating illegal bets exceeding 1.6 billion yuan (US $220 million).[74] Associated offshore Suncity operations were also identified by authorities taking place in jurisdictions including Australia, Cambodia, the Philippines, and Viet Nam, among others, with the syndicate extensively documented servicing major criminal groups around the world – particularly those engaged in cyber-enabled fraud and drug trafficking – alongside actors involved in hacking and sanctions evasion.[75,76]

In the aftermath of Suncity Group's collapse, authorities in Southeast Asia have observed a significant transformation in the regional threat landscape. The business model pioneered by Alvin Chau and the extended network of criminal investors and clients he led and serviced remains widespread and is proving more consequential than ever before. Underground banking and money laundering services once linked to the Group have not only consolidated but are fueling ongoing criminal expansion and innovation in other illicit markets in and beyond the region. This disruption has also generated a partial

70 Multiplier betting, also known as 'tok dai' (托底), refers to a form of 'under-the-table gambling' in which a bet formally denominated at the casino gambling tables only represents only a fraction of the total amount of a private bet made between gamblers and junket operators to avoid gaming revenue levies. It allows clients to pre-negotiate their preferred payment method, betting currency, and cash-out method while increasing the commissions received by VIP junket promoters, and can be used as a tactic to conceal the total amount of money transmitted through the casino by an individual bettor and obfuscate the source and destination of funds. Such arrangements are understood to have grown in popularity due to most junket customers in Macau SAR originating from mainland China. These customers do not—and in any case cannot—bring money with them to play due to strict capital controls and a nation-wide gambling ban in mainland China, and instead rely on credit issued by junket agents. For instance, should a customer request a HK $1 million credit, the junket agent can request the casino to provide HK $100,000 worth of chips, with the understanding between the junket agent and customer that a ten times multiplier is in effect.

71 Acusação do Ministério Público, n.º: 1345/2022.

72 China Central Television, Government of the People's Republic of China, January 2024.

73 Wenzhou City Public Security Bureau, 26 November 2021.

74 Shasi District Procuratorate of Jingzhou City, People's Procuratorate of HuBei, Press Release, September 2024.

75 Ibid.

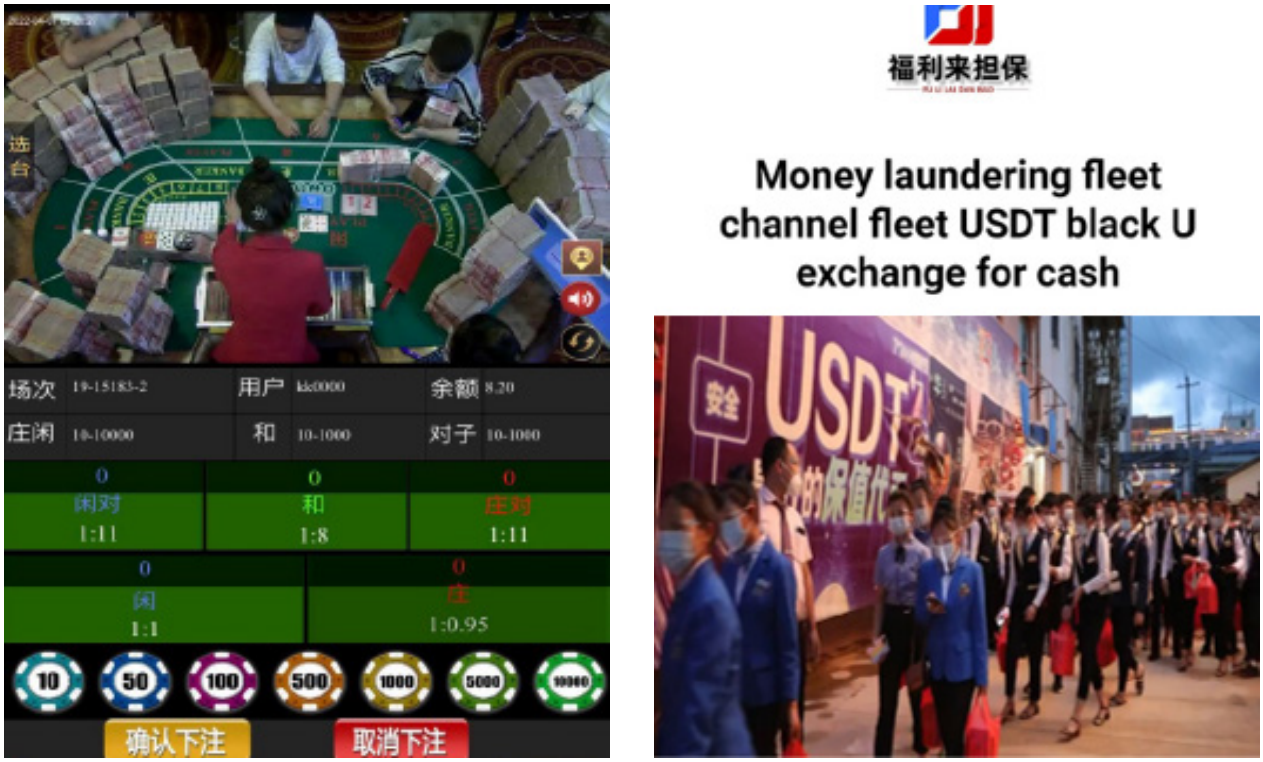
76 UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*.

power vacuum in its wake, drawing in a surge of new and old industry players who have sought to claim a portion of the underground banking business abdicated by Chau and Suncity.

Although the distribution of malware by an iGaming platform of BG 1's size is unprecedented by all accounts, this exceptional case is consistent with a broader trend which has seen illegal operators based in the region expanding their activities into various cyber and cyber-enabled crimes – providing further indication of powerful criminal networks based in Southeast Asia developing more advanced capabilities and maturing into more sophisticated cyber threat actors.

Rise of illicit online marketplaces in Southeast Asia

As examined in previous UNODC analysis,[77] one of the first major illicit online marketplaces observed in Southeast Asia was the Fully Light Guarantee. The platform was established by a large conglomerate owned and operated by the once powerful Liu family who were prominent within the leadership of the former Kokang Border Guard Force (BGF) in Special Region 1 (SR1) of Shan state, Myanmar, as well as Cambodia and other parts of the Mekong region and beyond.[78] Consisting of more than 350,000 users at its peak and supporting multiple scam centres, including those controlled by the Liu family in Kokang and Myawaddy, the platform was configured into numerous supply and demand channels dedicated to buyers and sellers engaged in money laundering and informal cross-border value transfer, people smuggling and recruitment, and various 'black' technological solutions and services advertised to cyber-enabled fraud syndicates. Similarly to the growing number of other Guarantee platforms operating in Southeast Asia today, Fully Light facilitated these activities through the creation of hundreds of public, private, and VIP groups and listings managed on behalf of paying vendors, with the marketplace guarantee serving as a backstop between buyers, sellers and service providers.



Screen captures of Kokang BGF hybrid gambling operations and money laundering platform. Source: Fully Light International, 2023.

In December 2023, the Criminal Investigation Bureau of the Ministry of Public Security of China issued ten arrest warrants for high-ranking members

77 See chapter on Kokang, Special Region 1 of Myanmar in: UNODC, Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia.

78 Ibid.

of the Kokang BGF leadership on charges relating to their roles in leading multiple violent criminal groups engaged in cyber-enabled fraud, drug production and trafficking, trafficking in persons, homicide, and money laundering targeting Chinese citizens.[79] Most of those charged were members of SR 1's Gambling and Entertainment Management Committee, and were overseeing various aspects of Kokang's online gambling, money laundering, and fraud industries, and several have been apprehended and currently face prosecution in China.[80]

As mentioned earlier, in February 2025, the Wenzhou Intermediate People's Court in East China's Zhejiang Province held a public first-instance trial for 23 defendants from another of Kokang's powerful families, the Ming family, which is alleged to have profited from gambling and fraud-related transactions exceeding 10 billion yuan (US $1.37 billion). According to prosecutors, the family exploited its influence in Kokang, using armed forces under its control to set up multiple cyber-enabled fraud parks in locations including Laukkai and Chinshwehaw which also harbored criminal financiers who were provided with armed protection. The trials of Fully Light International executives from Kokang's Liu family, among others, who have been documented engaging in similar illicit activities and generating billions of dollars per year in criminal proceeds,[81] are set to begin at a later date in 2025.

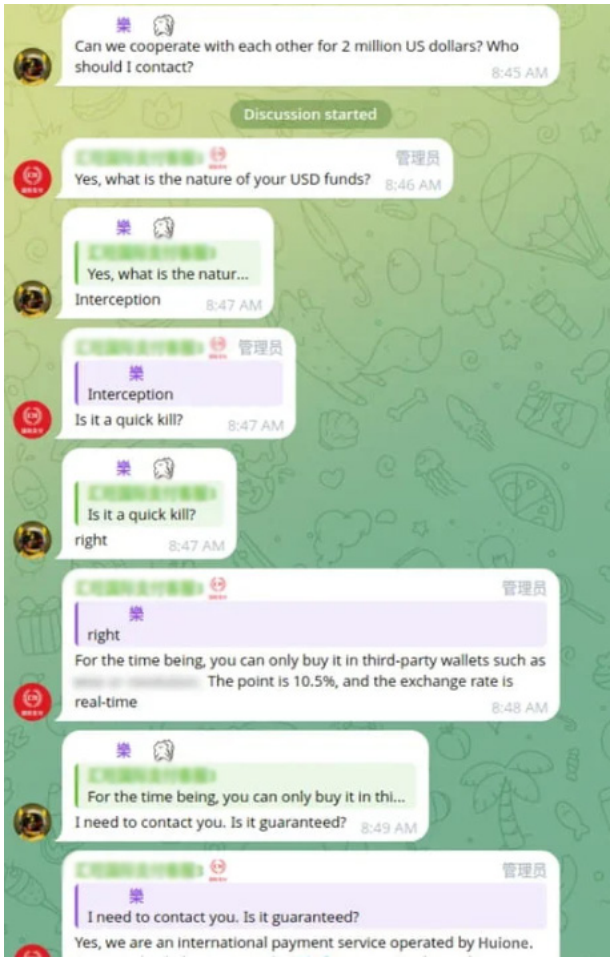
While the Kokang BGF was ultimately brought down by rival non-state armed group forces in January 2024, many other similarly configured 'guarantee' style marketplaces backed by criminal groups have launched throughout the region prior to and since their arrests. These new players have absorbed the majority of disrupted business which continues to grow and evolve at scale, posing threats to financial integrity, regional stability, and international security.

79 Criminal Investigation Bureau of the Ministry of Public Security, "Official WeChat", December 2023, available at: https://mp.weixin.qq.com/s/sm3wSWuxPSFcuSg4zlEfsQ.

80 Criminal Investigation Bureau of the Ministry of Public Security of the PR China, "The first trial of the Ming Family criminal group case begins", 19 February 2025, available at: https://mp.weixin.qq.com/s/uwPHS12Fj1PQiivdNlIDWg.

81 UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*.

Huione Guarantee: A Global Market Leader



A Huione Guarantee user inquires into services for laundering US $2 million obtained through a "quick kill". A representative of Huione International Payments, part of Huione Pay, responds, proceeding to set the terms and begin facilitating the transaction. Source: Elliptic (2024).

Over the past year, Huione Guarantee, now rebranded Haowang[82], has emerged as one of the world's largest illicit online marketplaces by users and transaction volume, representing a key piece of infrastructure fueling the expansion of Southeast Asia's cyber-enabled fraud ecosystem.[83] The predominantly Chinese-language platform was founded as an extension of the Huione Group of companies headquartered in Phnom Penh,

82 Huione Guarantee has tried to distance itself from Huione Group. For example the marketplace recently renamed itself to "Haowang Guarantee"[1]. Huione Group's payments business, Huione Pay also removed a section on its website dedicated to the marketplace and describing Huione Guarantee as a subsidiary. Despite this superficial distancing, Huione Guarantee confirmed that Huione Group remains a "strategic partner and shareholder".

83 Elliptic, "Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin", January 2025, available at: https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin.

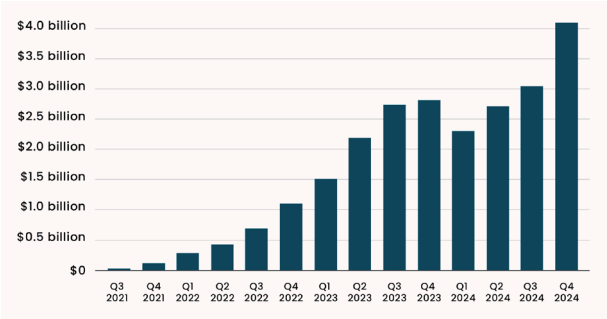
Cambodia, and has grown to more than 960,000 users and thousands of interconnected vendors at the time of writing. It is associated with current and former subsidiaries registered in countries including Canada, Poland, Hong Kong, China, and Singapore, and has notably shared platform administrators with the abovementioned Fully Light Guarantee, with which it shared a near exact platform design and business model.[84] Huione has also registered several trademarks currently active in the United States and elsewhere.[85]

Huione Guarantee has processed tens of billions of dollars in cryptocurrency transactions since 2021, with on-chain analysis indicating that the platform has become a one-stop-shop for illicit actors sourcing the technology, infrastructure, and resources needed to conduct cyber-enabled fraud and cybercrime, as well as evasion of sanctions under UN Security Council Resolutions.[86,87,88] This includes products and services such as targeted lists of stolen data, web hosting and mechanisms to ensure anonymity and bypass authentication on official app stores, money laundering and fund unfreezing specializing in specific jurisdictions and local financial institutions, compromised social media accounts, multimedia fraud content (scripts, photos, videos etc.), pre-registered SIM cards, and AI tools including sophisticated automation and deepfake software, among others. According to some expert estimates, cryptocurrency wallets used by Huione Guarantee and its vendors have received at least US $24 billion over the past four years, with an additional US $6 billion flowing through an associated Telegram bot used primarily for illegal online gambling which may be tied to further money laundering.[89]

Over recent years, Huione has also launched a range of its own cryptocurrency-related products including a cryptocurrency exchange, crypto-integrated online gambling platform, the Xone Chain blockchain network, and its own US Dollar-backed stablecoin which claims to be "…[un] restricted by traditional regulatory agencies" and designed to "avoid the common freezing and transfer restrictions of traditional digital currencies."[90] In February 2025, the Group announced its launch of the Huione Visa card, and has also noted making significant investments in other large illicit online marketplaces, social media and messaging platforms, and professional money laundering services, including acquiring a 30 per cent stake in the Tudao Guarantee in December 2024, highlighting how Huione may be hedging against future restrictions on its use of mainstream platforms.

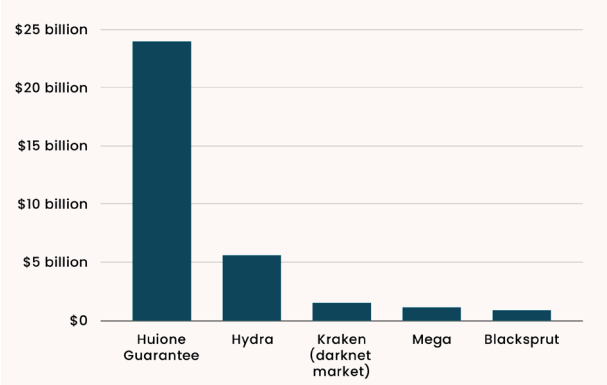
Law enforcement authorities and blockchain researchers have found Huione Guarantee and its vendors enabling fraud schemes targeting victims worldwide, generating billions in illicit proceeds and undermining efforts to establish trust in blockchain-based financial systems. For instance,

Figure 4. Value of cryptocurrency inflows received by wallets used by Huione Guarantee and its vendors, 2021 - 2024



Source: Elliptic, 2025.

Figure 5. Value of estimated cryptocurrency inflows of largest illicit online marketplaces of all time



Source: Elliptic, 2025.

84 UNODC, "Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat [restricted]", September 2023.

85 United States Patent and Trademark Office database, April 2025.

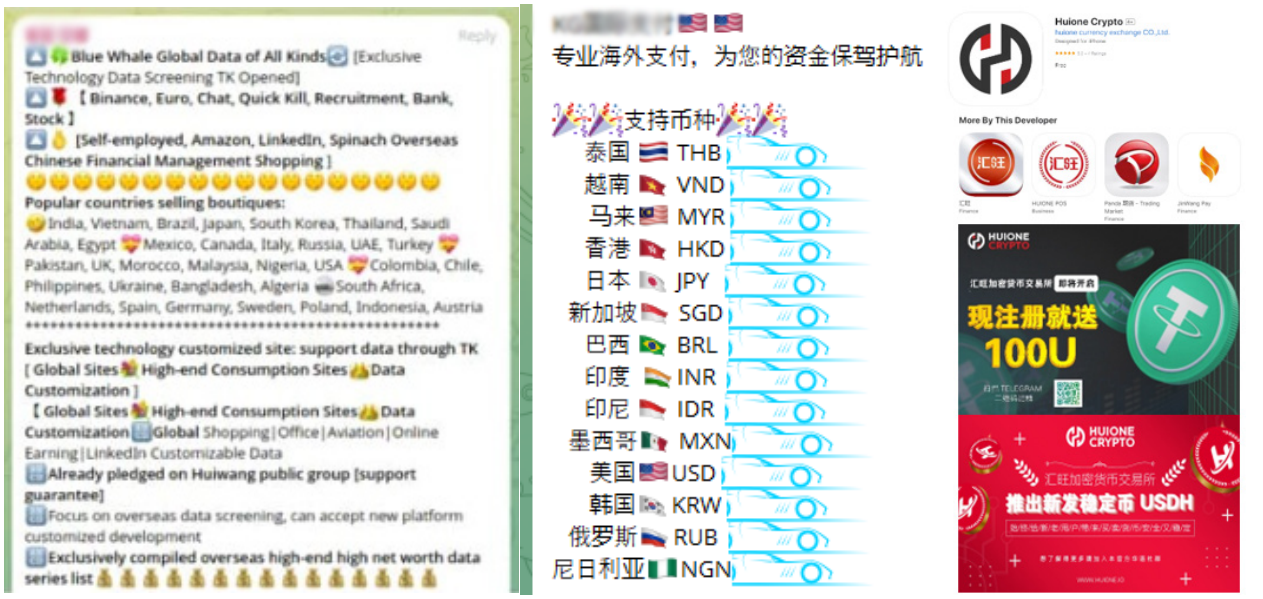
86 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in southeast Asia: A Shifting Threat Landscape*.

87 Elliptic, *Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin*.

88 Chainalysis, "Crypto Scam Revenue 2024", February 2025, available at: https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/.

89 Elliptic, *Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin*.

90 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in southeast Asia: A Shifting Threat Landscape*.



Listings of Huione Guarantee data vendor, Cambodia and U.S.-based 'motorcade' laundering service, and Huione Crypto mobile application, 2024.

in May 2024, two foreign nationals linked to cyber-enabled fraud and money laundering operations in Cambodia were indicted in the United States for laundering at least US $73 million in cryptocurrency investment scams through KG Pay, a Telegram-based money laundering service.[91] Examination of KG Pay administrator activity reveals extensive membership and use of Huione Guarantee and other rival marketplace platforms where multi-currency[92] laundering services targeting countries including the United States, Japan, and the Republic of Korea, were listed and explicitly advertised to criminal groups engaged in a broad range of cyber-enabled fraud.

Connections to Huione Guarantee money laundering services were further uncovered by blockchain experts in relation to a separate major cryptocurrency investment fraud campaign which victimized numerous US citizens, including the former CEO of the Kansas-based Heartland Tri-State Bank who was indicted on embezzlement charges for issuing US $47 million in wire transfers to Southeast Asia-based scammers, leading to the collapse of the bank. While the professional money laundering services utilized in this case remain unnamed at the time of writing, blockchain investigators have noted multiple connections to such services operating on Huione Guarantee visible through analysis of on-chain data.[93,94] Similar cases involving millions in stolen funds being deposited directly into Huione-controlled wallets have been reported by authorities in Australia, Canada, Europe, Japan, and elsewhere, highlighting the growing connectivity of the evolving criminal ecosystem in Southeast Asia as well as Huione's global impact.

Following months of growing international media attention driven by concerns raised from a range of blockchain and security experts, in January 2025 Huione Crypto was removed from the Google Play and Apple App stores. In March 2025, the National Bank of Cambodia, the country's central bank, confirmed it had withdrawn Huione's payment service institution license for non-compliance with existing regulations and recommendations.[95] Despite this effort, the company has continued to circumvent regulators and the decision has not appeared to have meaningfully disrupted Huione Guarantee nor its related cryptocurrency, payment, and shadow banking operations. In response, Huione Pay has denied all reports into its involvement in illicit activity and sought to distance itself from the Guarantee platform, however official information obtained through extensive analysis of historic DNS records as well as active trademark rights, among other data, confirm a direct connection between the two entities.

91 United States District Court for the Central District of California, "CR No. 2:24-cr-00311-SVW, Indictment", June 2023.

92 KG Pay offered services in currencies including Hong Kong Dollar, Japanese Yen, Korean Won, Malaysian Ringgit, Mexican Peso, Nigerian Naira, Russian Rubles, Thai Baht, and United States Dollar, among others.

93 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

94 Chainalysis, 2025.

95 Huione Group, "Official customer service channel" and press release, March 2025.

In March 2025, Huione Pay published a statement on its official Telegram channel stating that its international payment business has been transferred to Japan, where it has obtained a license and that Huione Canada would soon open. This message was later edited and a more formal statement was released in which Huione said its internationalization process was advancing, with payment and blockchain services in Japan, the Republic of Korea, and North America upgrading "providing customers with more extensive and high-quality services through decentralized wallets."[96] Examination of available business records confirms that the company has maintained a business license for its payment company in British Columbia, Canada, since October 2021.[97]

Following reporting on the withdrawal of its license, various WeChat media accounts active in Cambodia posted images of Huione customers rushing to the main office in Phnom Penh to withdraw funds. It is worth noting that Huione Pay increased interest rates paid out on all deposits of USDT from 2% to 7.3% in the wake of public reaction to its withdrawn banking license.[98] In December 2024, Huione Guarantee also announced its acquisition of a 30 per cent stake in another major Mekong-based online marketplace engaged in money laundering and informal cross-border transfer services. The renamed Haowang Guarantee[99] as well as recently registered Xone Investment websites, corresponding to Huione's new Xone blockchain network, have also migrated to a Lao PDR country code top-level domain.[100]

While Huione Guarantee and several similar platforms with clear links to organized crime in East and Southeast Asia continue to operate largely uninterrupted, they represent only a snapshot of the region's rapidly evolving criminal threat environment which should raise serious concerns among national authorities and the international community.

96 Ibid.
97 British Columbia Registry Service, "Huione Pay Inc", March 2025, available at: www.corporateonline.gov.bc.ca.
98 Huione Group, "Huione Pay application", March 2025.
99 Haowang Guarantee, "Website", available at: https://www.hwdb.la/.
100 Xone Investment, "Website", available at: https://www.xone.la/en.

Global expansion of East and Southeast asian criminal actors

Transnational organized crime groups based in Southeast Asia have proven adept at responding to increasing enforcement action targeting cyber-enabled fraud, money laundering, and underground banking. In response, these highly agile and entrepreneurial criminal networks have expanded and partially hedged against shifting regional dynamics, seeking out other jurisdictions with similar characteristics, opportunities, and vulnerabilities to target and exploit, driving intensifying global impact.

Criminal groups operating in and beyond the region have actively expanded their scope of operations, targeting an increasingly diverse range of victim profiles and nationalities from around the world -- both in the context of financial losses and trafficking for forced criminality. This has allowed Asian crime syndicates to dramatically scale up their profits while simultaneously generating vast reserves of illicit capital (fiat and cryptocurrency) that can be reinvested into existing operations and also utilized to service the underground banking and money laundering needs of other criminal groups globally using existing systems and infrastructure. In turn, criminal groups have also shown signs of expanding physical scam centre operations in several countries outside of the region.

Similarly to some of the most vulnerable parts of Southeast Asia, many countries beyond the region witnessing significant increases in illicit activity involving Asian crime syndicates face a variety of challenges in addressing the evolving situation. This ranges from limited human and technical resources (including forensic and investigative capacity), inter-agency coordination, international cooperation and intelligence sharing to cope with the scale of the problem, as well as high rates of corruption and low levels of legitimate foreign direct investment which criminal actors exploit.

As evidenced by recent trends and incidents examined in this section, public institutions in targeted countries also often possess low levels of awareness and understanding of emerging threats, crime types, modus operandi, and technologies leveraged by sophisticated Southeast Asia-based criminal groups, leaving many jurisdictions

vulnerable and underprepared. Developed countries with more robust capacity to address transnational crime have also proven susceptible and exposed to the ability of Asian criminal networks to infiltrate these jurisdictions by targeting gaps in anti-money laundering and due diligence frameworks, and utilizing complex shell structures and vast, increasingly digital underground banking systems to obfuscate the origins of their wealth and shift value across borders undetected.

Pacific Island Countries and Territories

Authorities in and around the Pacific region are increasingly reporting transnational organized crime groups originating from East and Southeast Asian countries are perceived to be among the most active in the Pacific Island Countries and Territories (PICTs).[101] In what appears to be part of a wider and interconnected trend, these networks have steadily expanded their influence in the Pacific in recent years through the development of casinos, junkets, hotel resorts, travel agencies, and other related businesses and investment projects, often involving virtual assets, used to conceal a wide range of illicit activities.

Similarly to their conduct in Southeast Asia, transnational organized crime groups operating in the Pacific often do so very openly, with some senior members appearing in public and presenting themselves as legitimate foreign investors in sectors that can be useful for their illicit businesses. Leaders of these networks have also proven effective in forming alliances with influential local figures in the Pacific region and leveraging these relationships, along with mutual financial interests, to advance their business networks and criminal activities.

To expand their presence in the Pacific, organized crime has increasingly targeted vulnerabilities relating to low levels of foreign direct investment, allowing them to advance their business interests and spread influence. They have also exploited citizenship-by-investment (CBI) schemes, particularly in Vanuatu, and have taken advantage of the region's low levels of enforcement capacity to address cyber-enabled crimes as well as foreign labour to import undocumented migrant workers.

Experts have observed that many investors and CBI applicants are often associated with complex webs of offshore businesses, with some owning shell companies with no discernible business activity.[102] Favourable shell company conditions have also been observed being targeted for illicit activity by foreign criminal actors in PICTs including the Republic of the Marshall Islands and Samoa.[103] Some criminal actors are also reported to have exploited diplomatic relations between their country of origin and the Pacific countries in which they operate, by falsely presenting themselves as working on behalf of their home government, as an important networking tactic used to obtain high level political access and preferential treatment.[104]

Recent incidents beginning in 2017 in various PICTs indicate that transnational organized crime groups centred in Southeast Asia have targeted the regional tourism industry and development of hotel resorts, concealing illegal online gambling and related trafficking in persons as well as incidents of suspected cyber-enabled fraud. This modus operandi, which has proliferated in Southeast Asia and various parts of the Pacific in recent years, has proven effective in providing organized crime with a cover and venue for illicit businesses including drug trafficking, money laundering, underground banking, and various forms of cyber-enabled crime. Signs of related criminal activities and operations have been observed in PICTs including Fiji, Palau, Samoa, Tonga, and the Commonwealth of the Northern Mariana Islands (CNMI) in recent years, with many confirmed links to the targeting of Vanuatu's CBI program by criminals associated with these activities.[105]

This crackdown followed observations made by the Office of the Special Prosecutor and the Foreign Investment Board of Palau, regarding numerous facilities appearing to be set up as call centers but which had no visible employees leaving or entering the premises, indicating involuntary confinement. The inter-agency operations resulted in the seizure of large amounts of laptop computers, cell phones, foreign SIM cards, bank tokens, and cash, and the discovery of more than 210 foreign nationals who

101 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact,* October, 2024..

102 Ibid.

103 Ibid.

104 Ibid.

105 Office of the Special Prosecutor of Palau, 2019-2020; UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*.

had been recruited into Palau on tourist visas from various countries in East and Southeast Asia and were suspected as being victims of trafficking in persons.[106]



Source: Office of the Special Prosecutor of Palau, 2020.

Official reports indicate that some of the undocumented laborers identified at the various sites had entered Palau via Cambodia and were suspected of being linked to online scam operations.[107] Authorities also noted several suspicious connections between the foreign owners of the raided facilities and both past and present Palauan officials as well as other local, influential facilitators.[108] As a result of information found during the execution of one of the related search warrants, it was further uncovered that the illegal online gambling operation in one of the raided venues had previously operated out of another hotel connected to senior 14K Triad members. This included OFAC-sanctioned Wan Kuok Koi[109], who has been linked to industrial-scale cyber-enabled fraud and money laundering operations throughout Southeast Asia and was highly active in Palau prior to his forced deportation by the Palauan Government.[110] According to the Office of the Special Prosecutor of Palau, this network had also managed to secure a preliminary 500,000 square meter land concession to develop a luxury beach resort in Angaur State, with documented plans to establish casino gaming operations.[111] Concerningly, it is also understood that several members of the 14K remain active on the island and have continued to expand their influence in Palau and elsewhere in the Pacific.[112]

A similar series of high-profile incidents highlighting the targeting of the PICTs by Asian criminal groups through casinos, resorts, and other related businesses, relates to former Saipan casino operator, Imperial Pacific International (IPI), a CNMI-based subsidiary of now delisted IPI Holdings in Hong Kong, China. Prior to its collapse, IPI was serially implicated in a range of criminal activities and investigations. In November 2023, this culminated in a ruling delivered by the Beijing Municipal First Intermediate People's Court, which convicted 14 individuals including the founders and senior IPI executives on charges relating to leading an organized criminal group, illegal casino operations, and smuggling of migrants, among other charges. Prior to this, in 2017, the Federal Bureau of Investigation (FBI) raided the IPI construction site in Saipan over a federal violation of the workplace visa system and systematic smuggling of migrants following the death of a construction worker in March that year. The FBI would go on to execute multiple search warrants on the company's offices between March 2018 and November 2019 in connection to a corruption probe involving the family of a former CNMI governor.[113]

106 Office of the Special Prosecutor of Palau, 2019-2020; UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*, p.29.

107 Office of the Special Prosecutor of Palau, 2019-2020; UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*, p. 29.

108 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*, p.29.

109 U.S. Department of the Treasury, "Treasury Sanctions Corrupt Actors in Africa and Asia", Press Releases, December 2020.

110 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*.

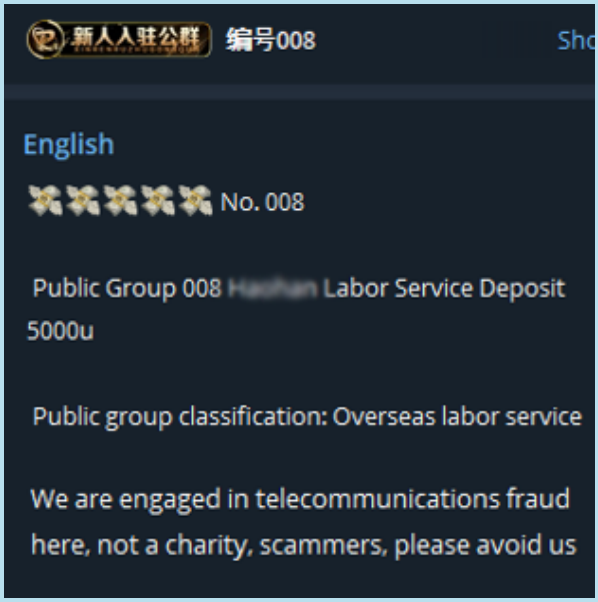
111 Ibid.

112 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*; UNODC consultation with regional experts.

113 United States Department of Justice, "Imperial Pacific International and MCC International Saipan Executives Indicted on Federal Charges Press Release", August 2020, available at: https://www.justice.gov/ opa/pr/imperial-pacific-international-and-mcc-international-saipan-executives-indicted-federal.

Launch of new 'Palau Guarantee' illicit online marketplace





Palau Guarantee illicit online marketplace and one listed service provider offering voluntary and trafficked labour supply for overseas scam centres identified by UNODC researchers. Source: Palau Guarantee.

The rise of new illicit online marketplaces servicing criminal groups based in Southeast Asia targeting victims globally represents a major shift within the regional threat landscape that has exacerbated existing challenges and fueled criminal expansion, with similar indications in parts of the Pacific. In February 2025, a new marketplace platform, Palau Guarantee, was launched on Telegram by a purported Cambodia-based network aiming to service overseas criminal actors. Consisting of more than 25,000 users at the time of writing, the Chinese-language marketplace is configured similarly to other major players in Southeast Asia, featuring sub-groups dedicated to money laundering, currency trading, and informal cross border value transfer, overseas labour and recruitment, citizenship-by-investment, visa, visa, so-called 'identity laundering' services, and cyber-enabled fraud materials. Palau Guarantee has also established a dedicated online gambling platform, Palau Entertainment, and has stated it will soon be launching a proprietary cryptocurrency wallet and token.

In August 2020, three IPI executives were indicted and ultimately convicted in the United States on federal criminal charges including a RICO conspiracy, harboring illegal aliens and unlawful employment of aliens for the purposes of building the Grand Mariana Casino and Resort, and international promotional money laundering.[114] The series of allegations and investigations into IPI's various criminal activities culminated in a November 2023 ruling delivered by the Beijing Municipal First Intermediate People's Court, which convicted 14 individuals including the founders and senior IPI executives on charges relating to leading an organized criminal group, illegal casino operations, and smuggling of migrants, among other charges.[115] Experts familiar with the case of IPI in Saipan have indicated that the criminal network continues to operate through a newly established hybrid (land-based and online) casino operation based on a neighbouring island in CNMI despite significant disruptions caused by recent enforcement action.[116]

Concerningly, in recent years there are other strong indications of criminality connected to IPI. For instance, IPI's founders were also controllers of the Hengsheng Junket, at one time among Macau's most capitalized and successful junket operators, which began to diversify its offshore casino and

114 Ibid.

115 Beijing Municipal First Intermediate People's Court, November 2023.

116 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*.

junket operations between 2013 and 2014 and establish satellite businesses in various parts of Southeast Asia.[117,118] In 2022, authorities in the Philippines reported rescuing a group of six Filipino nationals who had been unsuspectingly lured into a criminal operation where they were forcibly detained within the Hengsheng Casino in non-state armed group-controlled Kayin State, Myanmar, and ultimately trafficked.[119] The group was forced to engage in cyber-enabled fraud and released following large ransom payments made by their families.[120] The Hengsheng Junket also operated from a location in Poipet, Cambodia – another major hub for cyber-enabled fraud operations in the Mekong region – although its current status is unknown at the time of writing.[121]

Similarly to IPI, another major criminally implicated Mekong-based conglomerate has been observed dramatically increasing its investment portfolio in the Pacific in recent years, registering two large-scale property developments in Airai and Ngerbelas, Palau, and announcing plans for a third project through its subsidiaries.[122] According to regional law enforcement agencies, the Group possesses strong links to several cyber-enabled fraud compounds and money laundering operations including through illegal online gambling and cryptocurrency in Southeast Asia, with one court judgement estimating that illicit profits generated by its illegal gambling activities since 2016 exceeded 5 billion yuan (US $700 million).[123]



Source: Imperial Pacific International (top) and Hengsheng Casino (bottom), 2024.

117 The Stock Exchange of Hong Kong, “First Natural Foods Holdings Ltd.”, Company Filing, November 2023.
118 Donaco International, “Annual General Meeting - Chairman’s Address and Managing Director’s Presentation”, November 2015.
119 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact,* October 2024.
120 Ibid.
121 Ibid.
122 Pacific Economics, Investment Risk Brief, February 2025.
123 Wancang Country Court in Sichuan province of China, “Media Release”, July 2022, available at: http://gywcfy.scssfw.gov.cn/article/detail/2022/07/id/6792102.shtml.

Challenges of citizenship by investment in Vanuatu and connections to cyber-enabled fraud in Southeast Asia



CBI service provider advertisement showcasing Cambodian, Thai, Turkish and Vanuatuan passports in Bangkok prior to its removal by Thai government authorities (2024).

As highlighted by numerous high-profile cases around the world, criminal groups in Southeast Asia have increasingly targeted Citizenship By Investment (CBI) schemes in order to circumvent law enforcement, avoid extradition to their countries of origin, and hinder know your customer checks. This has been consistent with the rise of so-called "identity laundering" service providers explicitly marketing to foreign criminal groups fleeing prosecution, including those engaged in the regional cyber-enabled fraud and money laundering, as well as other serious crimes.

Regional criminal groups have frequently utilized Vanuatu's CBI program, alongside those in other countries outside of the Pacific, which are commonly advertised as a service within some scam centres in Southeast Asia. More particularly, agents within these compounds have been found to offer guaranteed CBI services to potential compound tenants who choose to invest and establish operations in these zones.[124]

In August 2024, for instance, authorities in Thailand reported the arrest of three Chinese nationals, including one wanted fugitive, who had entered the country on Vanuatu passports.[125] The group represented founding members of the 'Yingfa' criminal organization which established cyber-enabled fraud and illegal online casino operations in East and Southeast Asia and the Middle East, with the latter found to be processing a total of US $1.6 billion in illegal betting transactions as part of the money laundering process.[126]

Similarly, in August 2023, authorities in Singapore arrested 10 foreign nationals suspected of laundering an estimated SG $3 billion (US $2.3 billion) in overseas criminal proceeds generated from cyber-enabled fraud and illegal online gambling operations in Cambodia, Myanmar and the Philippines, representing the country's largest ever money laundering investigation.[127,128] All later pleaded guilty, surrendered assets and served short prison sentences. All 10 of the Chinese-born convicts each held multiple passports, including for Cambodia, Cyprus, Saint Kitts and Nevis, Dominica and Turkey, and three, Wang Shuiming, Su Wenqiang, and Su Jianfeng, held Vanuatuan citizenship, among others. Notably, Wang Shuiming, who was deported from Singapore to Japan following his 14-month prison sentence, visited Palau between December 2024 and January 2025 prior to his subsequent arrest in Montenegro.[129,130]

124 UNODC, *Transnational Organized Crime in the Pacific: Expansion, Challenges and Impact*.

125 Royal Thai Police, Bureau of Immigration, Press Conference, August 2024.

126 Ibid.

127 Singapore Police Force, "Ten Foreign Nationals to be Charged For Offences Including Forgery And Money Laundering With An Estimated Value Of About One Billion In Cash And Various Assets Seized, Frozen Or Issued With Prohibition Of Disposal Orders", 16 August 2023, available at: https://www.police.gov.sg/Media-Room/News/20230816_10_Foreign_Nationals_Offences_ Forgery_Money_Launder_Est_1_Bil_Assets.

128 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.*

129 Pacific Economics, Investment Risk Brief, February 2025.

130 Police Directorate of Montenegro, Media Release, February 2025.

Japan's exposure to online gambling, cyber-enabled fraud and money laundering

Japan is deeply impacted by the expansion of the regional cyber-enabled fraud and online gambling industries, and funds from both are known to flow illicitly into and out of the country.

Arrests have been made across the region of Japanese nationals allegedly involved in cyber-enabled fraud activity, including in the Philippines, Thailand, Myanmar, and Cambodia. Japanese police have cooperated with local law enforcement with intelligence sharing, and in several cases have travelled to receive arrested citizens who have been arrested on return flights to Japan. For example, in April 2023, 19 Japanese nationals were arrested in Sihanoukville and 25 more following a raid on a scam operation in Phnom Penh, all of whom were deported and arrested.[131]

Japanese nationals have also been trafficked into the industry, and following the raids in Myawaddy in February, 2025, it emerged that several Japanese minors were trapped in scam compounds in the area.[132] Japan's Ministry of Foreign Affairs has issued multiple warnings to citizens from at least 2023 regarding fraudulent recruitment into forced scam work in Myanmar.[133]

Losses to online fraud including investment and romance scams in Japan spiked in 2024, increasing more than 50 per cent in the previous year. Many of these losses will likely be the result of fraud originating from the region.[134] This includes investment scams, 'pig-butchering', romance scams, law enforcement impersonation, and extortion of the elderly with fake pension and health insurance products. Additionally, in March, Japan's National Police Agency released the results of a survey that estimated 3.37 million Japanese have used overseas online casinos, spending ¥1.2 trillion on illegal gambling annually.[135]

In Thailand several arrests of alleged senior crime bosses with links to cyber-enabled fraud occurred in 2023 to 2024. One such case took place in December, when Thai police raided luxury villas in Pattaya and arrested the alleged leader of a scam gang targeting elderly Japanese. Thai authorities described him as a former member of the Yamaguchi-gumi yakuza syndicate.[136] Other more recently established crime groups have also been identified in the region operating illegal gambling and fraud operations, including the Luffy syndicate, whose leaders were arrested and deported from the Philippines in recent years.[137,138]

Japanese money laundering groups have established platforms and cooperate with regional groups to move proceeds of these illegal industries, for example, in 2024, Japanese authorities brought down senior members of the Rivaton Group (リバトングループ), a money laundering organization found to have deposited at least ¥70 billion (US $487 million) in illicit funds into over 4,000 corporate accounts associated with more than 500 front companies.[139] At least 40 people worked for the group, and under pursuit by authorities, its leaders fled to the Southeast Asia region and in July and August two were arrested in the Philippines.[140] Three others were arrested later after flying back to Japan.[141,142]

131 Global Fraud Meeting, National Police Agency of Japan, Tokyo, Japan, September 2024.
132 Royal Thai Police, "Stakeholder Roundtable Closed-Door Meeting", Bangkok, Thailand, February 2024.
133 See for example: Ministry of Foreign Affairs of Japan, "Beware of Fraud Sites Near the Myanmar-Thailand Border (Thailand)", 27 February 2025, available at: https://www.anzen.mofa.go.jp/info/pcspotinfo_2025C006.html; Ministry of Foreign Affairs of Japan, "Warning About Special Fraud Cases (How to Avoid Becoming a Perpetrator (Part 3)", 20 February 2025, available at: https://www.anzen.mofa.go.jp/info/pcwideareaspecificinfo_2025C003.html.
134 Japan National Police Agency, "Status of Awareness and Arrest of Special Fraud and SNS-based Investment and Romance Fraud", available at: https://www.npa.go.jp/publications/statistics/sousa/sagi.html.
135 The Japan Times, "3.37 million in Japan use overseas online casinos, police survey suggests", 13 March 2025, available at: https://www.japantimes.co.jp/news/2025/03/13/japan/japan-online-gambling-police-survey/.
136 Thai Immigration Bureau, Press Conference, 18 December 2024.
137 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.
138 Bureau of Immigration, "BI agents arrest Japanese fugitive", 7 March 2024, available at: https://immigration.gov.ph/bi-agents-arrestjapanese-fugitive/.
139 Japan National Police Agency, Media Release, 23 May 2024.
140 Philippines Bureau of Immigration, "BI to deport Jap fugitive wanted for fraud, money laundering", 28 August 2024, available at: https://immigration.gov.ph/bi-to-deport-jap-fugitive-wanted-for-fraud-money-laundering/
141 Osaka Prefectural Police, Media Release, September 2024.
142 Global Fraud Summit, National Police Agency of Japan, Bilateral Meeting, Tokyo, Japan, September 2024.

Africa

Several African countries have long had their own scam industries, but in recent years there have been increasing indications of operators from East and Southeast Asia establishing bases in various countries on the continent, potentially taking advantage of similar conditions that made Southeast Asia a suitable base for the expansion of the industry.

Beginning in early 2024, reports have started to emerge of significant operations being identified by law enforcement across Africa. For instance, in April 2024, a fraud syndicate was discovered in Zambia, leading to the arrest of 77 suspects, including 22 Chinese nationals who were later sentenced to up to 11 years in jail for leading the operation.[143] Elsewhere, Nigeria has shown signs of emerging as an important destination for groups diversifying into Africa. A major raid occurred in December 2024 in Lagos that led to the arrest of almost 800 people.[144] Among them were 148 Chinese nationals and 40 Filipinos. According to Nigeria's Economic and Financial Crimes Commission (EFCC), they are suspected of involvement in cryptocurrency investment and romance scams. The EFCC stated that the foreign nationals trained Nigerian accomplices, further demonstrating the corrupting influence of the industry. In the following months, dozens of the suspects were arraigned on charges under financial and cybercrime laws.

The EFCC led further raids on online scam operations in January arresting 101 people, including four Chinese nationals.[145] Responding to the rise in Chinese involvement in financial crimes in Nigeria, the Chinese Ambassador met with the EFCC in March to discuss the potential for sending a working group to train Nigerian counterparts in evidence collection and fraud tracing.[146] In late 2024, there were also reports of significant raids in Angola in which dozens of Chinese nationals were detained for alleged involvement in online gambling and fraud,[147] and in 2023, nine Chinese, three Namibians, a Singaporean and a Cuban were arrested for allegedly operating a 'pig butchering' scam in Namibia.[148]

The Philippines Department of Migrant Workers released a statement saying the Filipinos detained in the Lagos raids were recruited from Dubai.[149] This follows a trend identified by anti-trafficking groups, who have seen cases of UAE-based foreign workers of various nationalities being lured into scam work in Southeast Asia, and further indicates that Dubai is becoming a global hub for recruitment and trafficking linked to the cyber-enabled fraud industry.[150] Testimonies from numerous people rescued from scam sites in Southeast Asia, including Africans, have revealed they were working in Dubai when they were recruited online, often with offers of IT or customer service jobs in Thailand, then trafficked to neighbouring countries.[151] As noted earlier, as the workforce in Southeast Asian operations has diversified, Africans are increasingly being found in online compounds in the region. Movement between the two continents now appears to be two-way, and law enforcement agencies have reported concerns over 'professional scammers' returning to African countries.[152]

143 Drug Enforcement Commission of Zambia, April 2024.

144 Economic and Financial Crimes Commission, "EFCC Bursts Syndicate of 792 Cryptocurrency Investment, Romance Fraud Suspects in Lagos … Arrests 193 Chinese, Arabs, Filipinos, Others", 16 December 2024, available at: https://www.efcc.gov.ng/efcc/news-and-information/news-release/10584-efcc-bursts-syndicate-of-792-cryptocurrency-investment-romance-fraud-suspects-in-lagos-arrests-193-chinese-arabs-filipinos-others.

145 Economic and Financial Crimes Commission, "EFCC Arrests 105 Suspected Internet Fraudsters in Abuja", 10 January 2025, available at: https://www.efcc.gov.ng/efcc/news-and-information/news-release/10605-efcc-arrests-four-chinese-101-others-for-suspected-internet-fraud-in-abuja.

146 Economic and Financial Crimes Commission, "Chinese Working Group to Collaborate with EFCC in Tackling Cybercrime", 4 March 2025, available at: https://www.efcc.gov.ng/efcc/news-and-information/news-release/10755-chinese-working-group-to-collaborate-with-efcc-in-tackling-cybercrime.

147 Angola24horas, "Chineses detidos em Luanda por gestão fraudulenta de mais 400 jogos 'online'", 28 August 2024, available at: https://angola24horas.com/sociedade/item/30310-chineses-detidos-em-luanda-por-gestao-fraudulenta-de-mais-400-jogos-online; Angop, "National Police arrest social media scammers in Luanda", 21 October 2024, available at: https://angop.ao/en/noticias/sociedade/detidos-cidadaos-chineses-por-criacao-de-perfis-falsos-para-burlas-nas-redes-sociais/.

148 Namibian Police Agency, Media Release, September 2023.

149 Department of Migrant Workers, "DMW warns OFWs vs 'third country recruitment'", 13 January 2025, available at: https://dmw.gov.ph/news-releases/2025/DMW-warns-OFWs-vs-third-country-recruitment.

150 Humanity Research Consultancy, "Uncovering the Spread of Human Trafficking for Online Fraud into Laos and Dubai", July 2024, available at: https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/66bec89de33fb0311442d888_Asia-CTIP%20Laos%20Dubai%20Investigation.pdf.

151 Information provided in meetings with regional anti-human trafficking organizations and other stakeholders..

152 Japan National Police Agency, Global Fraud Meeting, Tokyo, Japan, September 2024.



Suspects held after arrest in Lagos, December 2024. Source: Economic and Financial Crimes Commission.

There have been indications for several years of Asian organized crime actors establishing connections to the African continent. One example is that of Liu Dawei, a native of Tangshan in northern China who established a business empire in Cambodia's Sihanoukville via his Goddess of Liberty Group. Earlier, in 2009, Liu had been sentenced to time in jail in Tangshan for leading a criminal group, facilitating underground gambling, organizing people to travel to the Philippines for online gambling work, and various other offences.[153]

Between 2016 and 2021, Liu Dawei registered more than 10 companies in Cambodia under his birth name or as Michael Liu[154] (the name he acquired after receiving Cambodian citizenship), and was associated with several more.[155] After opening a large casino on the Cambodian coast, the group announced it was also developing large-scale casino properties in Myanmar's Myawaddy,[156] although it is unclear whether they were completed. Reports indicate that Liu fled Cambodia to evade apprehension, but in 2021 it was reported that he was arrested in Uganda on an Interpol Red Notice along with three associates and deported to China.[157] The following year, the Nan'an City Public Security Bureau published a notice seeking information from the public related to the activities of Liu Dawei and his organization to aid their investigations into alleged kidnapping, extortion, intentional injury, and illegal detention, among other offences.[158]



Reports of Liu Dawei's arrest, December 2021. Source: Uganda New Vision.

In Cambodia, the Goddess of Liberty Group had connections to the World Hongmen History and Culture Association.[159] The founder and head of the association is longtime senior 14K triad member, Wan (Broken Tooth) Kuok Koi. In December 2020, Wan was designated by the U.S. Treasury Office of Foreign Assets Control as a triad leader and his companies as engaging in various criminal activities including drug trafficking, trafficking in persons, and illegal gambling.[160] He is believed to be a key investor in casino and cyber-enabled fraud compounds in and around Myawaddy, Myanmar, through his Hong Kong, China-registered Dongmei Group, alongside related businesses in other neighbouring countries.[161] At the same time, the World Hongmen History and Culture Association has also been reported increasing activity in Uganda and other African countries in recent years.[162]

153 Yanzhao Metropolis Network, "A gang involved in organized crime in Hebei Province is equipped with finger cutting knives", 25 May 2010, available at: https://news.sohu.com/20100525/n272329187.shtml [can only find media reports, but this is a Party newspaper]

154 According to naturalisation decree in Cambodia's Royal Gazette, December 2018.

155 According to Cambodia's Ministry of Commerce Business Registry.

156 Reported in posts on the company's now deleted WeChat account in 2020.

157 Uganda Police Force, Official Media Release, December 2021.

158 Nan'an Public Security Bureau, "Notice on Publicly Soliciting Clues Regarding the Crimes Committed by Liu Dawei and Others", 18 March 2022, available at: https://mp.weixin.qq.com/s/LEfwqC7oP0CECaPbCDBblg.

159 Paid-for promotional articles published by local media covering Goddess of Liberty events referred to the company's chairman and president respectively as president and secretary general of the Cambodian branch of the Hongmen association. For example, see: Cambodia-China Times, "Cambodian Goddess of Liberty Group and Others Donate to Extremely Poor Families", 18 August 2021, available at: https://cc-times.com/posts/15051.

160 U.S. Department of the Treasury, "Treasury Sanctions Corrupt Actors in Africa and Asia", December 2020, available at: https://home.treasury.gov/news/press-releases/sm1206.

161 UNODC, *Casinos, Money Laundering, Underground Banking and Transnational Organized Crime in East and Southeast Asia*.

162 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.*

Clandestine cryptocurrency mining operation in militia-controlled territories of Libya[163]

Unlike traditional cryptocurrency exchanges, crypto mining typically falls outside the scope of anti-money-laundering authorities and can provide illicit actors with a stream of steady and nearly anonymous revenue. Illegal crypto mining operations provide organized crime groups with a powerful tool for generating and laundering illicit funds while minimizing detection risks. Criminal groups establish unauthorized mining farms, often relying on stolen electricity.[164] This can allow them to mine cryptocurrencies at little to no cost, creating untraceable digital assets with no direct ties to criminal activities.

Since mining rewards do not face high levels of regulatory and enforcement scrutiny in many targeted jurisdictions, criminals can seamlessly introduce dirty money into the financial system by generating seemingly lawful earnings. This can take place through reinvestment of illicit funds obtained from criminal activities into mining farms requiring expensive, high-powered mining rigs, large, ventilated facilities, and staff to manage clandestine mining operations. The mined cryptocurrency can then be sold, transferred, or exchanged, further obscuring its origins and enabling criminals to convert illicit gains into clean, usable assets.

In recent years, illegal cryptocurrency mining has emerged as a significant concern across the Middle East and Africa, driven by low electricity costs, weak regulatory frameworks, and increasing digital financial adoption.[165] Governments have attempted to crack down on illicit mining; however, enforcement challenges persist as foreign operators and organized criminal groups continue to exploit these regulatory and enforcement gaps.

In June 2023, Libyan authorities dismantled a major illegal cryptocurrency mining operation in Zliten, a city 160 kilometers east of Tripoli.[166] The raid led to the arrest of 50 Chinese nationals found operating a sophisticated mining farm within an abandoned iron factory.[167] The facility was equipped with high-powered computers, digital conversion systems, and high-voltage refrigeration units, consuming vast amounts of electricity.[168] The operation was entirely off-grid, bypassing Libya's power infrastructure and using illegally acquired energy.[169]



Images of the raided illegal cryptocurrency mining sites in Libya. Source: Attorney General's Office of Libya and Law Enforcement Department of the General Department of Security Operations of Libya, 2023.

This case was part of a broader crackdown, following a similar raid in Misrata, where 10 Chinese nationals were arrested for unauthorized mining activities.[170] These incidents underscore the growing role of foreign actors—particularly from East Asia—in Libya's illegal cryptocurrency mining sector, with various risks emerging around this type of activity related to transnational organized crime. Such networks are known to operate across jurisdictions, often exploiting regulatory blind spots and leveraging technical expertise to scale operations with minimal traceability.

163 The Libya Observer, "Attorney General's Office", 2024, available at: https://libyaobserver.ly/tag/attorney-generals-office; Law Enforcement Department of the General Department of Security Operations of Libya, "Press release", 2024.

164 Metropolitan Electricity Authority of Thailand, "MEA invites people to report suspected electricity theft for bitcoin mining, imposing maximum penalties on illegal miners", September 2024, available at: https://www.mea.or.th/en/public-relations/corporate-news-activities/announcement/VkwGjlBg5.

165 Domain Name System (DNS) is a protocol that translates domain names into numerical IP addresses, enabling computers to locate and communicate with each other over the internet.

166 Agence France-Presse, "Libya Arrests 50 Chinese Nationals in Crackdown on Crypto Mining", June 2023, available at: https://www.voanews.com/a/libya-arrests-50-chinese-nationals-in-crackdown-on-crypto-mining/7149715.html

167 Law Enforcement Department of the General Department of Security Operations of Libya, June 2023.

168 Attorney General's Office of Libya, June 2023.

169 Ibid.

170 Agence France-Presse, *Libya Arrests 50 Chinese Nationals in Crackdown on Crypto Mining*; Attorney General's Office of Libya, June 2023.

Libya's appeal to illegal miners stems from its extremely low electricity prices, estimated at just $0.008 per kilowatt-hour—one of the cheapest rates globally, behind Iran, Ethiopia, Syria, Cuba, and Sudan.[171] This affordability has made Libya an attractive destination for miners seeking to maximize profits. The scale and sophistication of certain operations—often established in remote areas using off-grid power sources—have raised concerns about the possible involvement of transnational organized crime groups. The unregulated expansion of mining operations has significantly contributed to chronic power shortages in parts of Libya, leading to blackouts lasting up to 24 hours.[172] The Libyan government has cited illicit mining as a direct cause of electricity supply failures, as unauthorized mining farms consume vast amounts of power, depriving essential services and residential areas.[173] This major incident reported by Libyan authorities reflects a broader pattern seen in several African and Middle Eastern countries, where illegal cryptocurrency mining and related crimes are on the rise. While information remains limited, the trend suggests growing risks linked to money laundering and organized crime, prompting government action across the region.

171 Statista, "Least expensive household electricity prices worldwide in December 2023, by select country", July 2024, available at: https://www.statista.com/statistics/1391069/cheapest-residential-electricity-by-country-world/

172 Ahmed Elumami and Ayman Al-Warfali, "Libya's power cuts enrage citizens, spurring protest", Reuters, July 2022, available at: https://www.reuters.com/world/africa/libyas-power-cuts-enrage-citizens-spurring-protest-2022-07-04/

173 Sky News Arabia, "After Dbeibah's speech... What is the relationship between Bitcoin and the electricity crisis in Libya?", July 2022.

Indication of other ongoing expansion

South America

Recent trends and incidents indicate that transnational organized crime groups from Asia have increasingly expanded into and targeted various parts of South America. While data remains limited in comparison to other regions, Asian criminal networks have been observed scaling up their South American-facing online operations and infrastructure.[174] This has been particularly noticeable in the case of cyber-enabled fraud and illegal online gambling platforms in past years, leading to a parallel increase in demand for Spanish and Portuguese speaking labour within Southeast Asian scam centres.[175] These crime groups have also sought to enhance critical money laundering and underground banking partnerships with major South American drug trafficking organizations or cartels and, in a number of isolated cases, have managed to establish physical scam operations locally.

For instance, in October 2023, Peruvian authorities rescued a group of over 40 Malaysians including 26 women and 17 men who were trafficked by a gang from Taiwan PoC identified as the Red Dragon (Dragón Rojo) syndicate and forced to commit cyber-enabled fraud.[176] During the investigation, victims testified to being recruited on Facebook by a Malaysian national to work in casinos and hotels in Lima, expecting compensation between US $2,000 to $3,000 a month.[177] Upon arrival, their passports and belongings were confiscated by the gang which forced them to conduct police impersonation scams targeting people in Malaysia, Indonesia, Thailand, the Philippines and Singapore from a luxury residence in La Molina.[178] Investigators identified a naturalized Ecuadorian businessman born in Taiwan PoC as the leader of the operation.[179]



Rescued Malaysian victims and Red Dragon gang members detained by Peruvian authorities.
Source: Peruvian National Police, October 2023.

174 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.*

175 Japan National Police Agency, "Global Fraud Meeting", September 2024.

176 Peruvian National Police, Official Media Release, October 2023.

177 Ibid.

178 Ibid.

179 Ibid.

Beyond this recent incident, it is notable that Brazil has emerged as one country that has faced a growing set of challenges related to cyber-enabled fraud, online gambling, and related money laundering, with some linkages to criminal groups operating in Southeast Asia. Authorities in Brazil have also noted a growing trend involving the trafficking of Brazilian nationals into Southeast Asia for forced criminality, with such cases representing the vast majority of all trafficking in persons cases reported by Brazilian authorities involving the country's nationals in recent years.[180,181] This development is consistent with data suggesting growing targeting of Brazilians by cyber-enabled fraud and illegal online gambling operators based in Southeast Asia.

Most recently, the situation reached a peak in public awareness following the rescue of two young Brazilian men who were deceived by fake job ads and trafficked into a scam centre in Myawaddy, Myanmar, upon arriving in neighbouring Thailand. Both victims were forced to commit scams targeting other Brazilians and regularly beaten, with one of the two men reportedly being detained in a dark room over a prolonged period of time for non-compliance. Many other Brazilians are understood to remain trapped or voluntarily engaged in other scam centres in Myanmar and elsewhere in the region.[182]

Brazil has also increasingly faced challenges related to illegal online gambling platforms targeting its nationals, with authorities finding related transactions often operated beyond the purview of Brazil's financial regulator and suspecting that many operators deploy manipulated software to boost profits. The situation has ultimately led the country to decriminalize and regulate the industry in January 2025. To de-risk the new regulatory regime, in late 2024 the Brazilian Senate authorized the creation of a select committee to investigate money laundering on sports betting platforms, as well as the influence of illegal online gambling on the economy and its facilitation of organized crime.

While Brazil has now licensed numerous online gambling platforms and service providers, several platforms linked to major criminal networks in Southeast Asia associated with cyber-enabled fraud have been observed targeting the country. In 2023, convicted money launderer, Su Baolin, was alleged by Singaporean authorities investigating the country's largest ever money laundering case to be operating illegal gambling websites in Myanmar targeting users in Brazil and China.[183] Investigators identified between US $5 million to $6 million in profits connected to these operations between 2020 and 2022 paid in USDT cryptocurrency through intermediaries in Dubai, with the case linked to various online gambling and scam centres operating in Cambodia and the Philippines.[184]

Brazil has also been targeted by Asian crime syndicates engaged in illegal online gambling and cybercrime operations from beyond Southeast Asia. Most recently, in August 2024, authorities in Luanda, Angola reported dismantling an international criminal network operating illegal online gambling and phishing operations targeting Brazilian and Nigerian bettors, arresting 46 Chinese nationals and 113 local Angolans and seizing 223 computers and 113 mobile phones.[185] According to investigators, the operation consisted of more than 400 online games, many of which distributed malware designed to harvest and steal user data including banking credentials and other sensitive and personal identifying information.[186]

As Asian crime syndicates continue to diversify their targeting and scope and seek to develop new revenue streams in underexplored markets, it is clear South America presents many opportunities – with recent developments suggesting the current situation is likely to intensify on the continent.

180 Royal Thai Police, Stakeholder Roundtable Closed- Door Meeting, Bangkok, Thailand, February 2024.
181 Ibid.
182 Ibid.
183 Singapore Police Force, Commercial Affairs Department, December 2023.
184 Ibid.
185 Andora Serviço de Investigação Criminal, August 2024.
186 Ibid.

Growing impacts of enhanced collaboration between Asian money laundering organizations and criminal groups abroad

Over the last few years, law enforcement agencies from around the world have reported on expanding collaboration, partnerships, and synergies forming between Asian money laundering organizations (MLOs) and criminal groups from around the world including South American drug cartels, the Italian mafia, and Irish mob, among many others. This trend has largely been driven by enhanced enforcement of strict capital controls in some countries in East and Southeast Asia which has fueled demand for foreign currency as well as innovation in systems and mechanisms to move and transfer value across borders undetected. In recent years, it was also accelerated in response to past restrictions on cross-border movement of goods and people which took place during the COVID-19 pandemic and disrupted bulk cash smuggling networks, forcing criminal groups to urgently adopt new business models and strategies.

The growing supply of criminal proceeds in need of laundering has aligned with the unprecedented demand for foreign currency within underground banking markets in Asia, presenting major opportunities and incentives for criminal networks based in East and Southeast Asia to expand their informal and often illicit money services internationally. The impact of this shift has proven highly consequential for governments both within and beyond the region, enabling transnational organized crime groups to scale up their illicit activities by dramatically reducing the cost of money laundering and improving the speed, efficiency, and anonymity with which it can take place. At the same time, the situation has afforded unprecedented access to highly sought-after reserves of illicit foreign capital for Asian crime syndicates expanding globally, fueling the system's self-sustained growth while increasing the utility of criminal proceeds amassed by organized crime in Southeast Asia – with many major syndicates deploying huge reserves of illicit capital to establish integrated casino resorts, junkets, online gambling platforms and, increasingly, unregulated financial service businesses engaged in banking, payment processing, and both foreign and cryptocurrency exchange used to service transnational organized crime globally.

One of the best documented examples highlighting this trend and its accelerating global impact relates to enhanced collaboration between Mexican drug cartels and Chinese MLOs, which has been extensively reported by authorities in North America in recent years. According to officials, the outsourcing of money laundering activities by the cartels to professionals with extensive ties to Asian criminal networks has increased difficulties to trace and disrupt associated illicit financial flows.[187] Unlike other professional launderers who may charge higher commissions for their services, Chinese MLOs and brokers have been found to undercut the competition by charging between 0 to 6 per cent, making their profit by reselling foreign currencies – in this case U.S. dollars generated by the cartels – to overseas buyers who are willing to bear the majority of the service cost.[188] Moreover, the diversification of laundering techniques by Chinese and other Asian criminal networks, including those utilizing mirror transactions[189], international networks of money mules or so-called motorcades,[190] as well as casino junkets, online gambling,

187 U.S Department of the Treasury, "Treasury Sanctions Mexico- and China-Based Money Launderers Linked to the Sinaloa Cartel", 1 July 2024, available at: https://home.treasury.gov/news/press-releases/jy2439; UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

188 U.S. House Committee on Oversight and Accountability Subcommittee on Health Care and Financial Services, "China in Our Backyard: How Chinese Money Laundering Organizations Enrich the Cartels", 26 April 2023, available at: https://oversight.house.gov/wp-content/uploads/2023/04/Hearing-on-Chinese-Money-Laundering-Mavrellis-Written-Testimony-4.26.2023-FINAL.pdf.

189 Mirror transactions involve cross-border currency swaps. In these transactions, an intermediary usually receives one currency (e.g., accepts U.S. dollars earned by local drug dealers) and deposits an equivalent amount of another currency in a foreign bank. These types of schemes, which may also integrate trade-based money laundering methods and cryptocurrencies, offer a mechanism for cartels and other criminal groups to access criminal profits rapidly and with greater anonymity while limiting exposure and risk.

190 Motorcades or fleets refer to networks of organized money mules offering pass-through services used by organized crime to impede financial investigations by routing money through multiple bank or cryptocurrency exchange accounts for a percentage of the total funds transferred. It has been observed that a common practice among large motorcade teams is to collaborate with others when processing larger contracts, enhancing both concealment and effectiveness. Regional law enforcement has also reported the use of illegal online gambling platforms to further obfuscate the source of funds processed in this way.

cryptocurrencies, and related service providers, has further compounded existing challenges.

Major cases reported by international law enforcement frequently include the use of cash couriers associated with Asian MLOs who coordinate with local criminal groups to systematically collect their criminal proceeds, with some recent incidents in the United States revealing bi-weekly exchanges of amounts ranging between US $150,000 to $1 million per pickup.[191,192,193] In July 2024, U.S. authorities working with authorities in China and Mexico dismantled another major transnational criminal operation involving members of the Sinaloa Cartel and a Chinese money laundering network involving the facilitation of large-scale distribution of cocaine, methamphetamine, and fentanyl across the United States. Defendants named in the indictment were alleged to have orchestrated bulk cash pickups using coded communications and structuring deposits through multiple operatives to evade financial reporting requirements. Large sums were either transferred via cryptocurrency or funneled through associated shell businesses and real estate transactions. The network is believed to have moved more than US $50 million in drug proceeds between 2019 and 2023.

In another major example, between 2008 and 2019, Xizhi Li, a Chinese businessman with U.S. citizenship, together with Asian criminal associates operating in Belize, China, Guatemala, Mexico, the United States, and elsewhere, laundered nearly US $30 million of drug proceeds for Mexican, Colombian, and Guatemalan drug trafficking organizations via a casino in Guatemala, a U.S. seafood export company, and U.S., Chinese, and other bank accounts as well as cryptocurrency.[194] As described in Figure 6 below, bulk drug cash would be collected by the network and later deposited into bank accounts, with the funds sold to overseas buyers and corresponding value (currency and/or goods) transferred to the cartels.

It is worth noting that one of the convicted co-defendants in this matter was additionally found to have bribed an undercover investigator using cryptocurrency to obtain U.S. passports, and was implicated in a multi-million-dollar cryptocurrency investment fraud as well as potential financial connections to sanctioned entities.[195] The same individual also acquired a majority stake of a New York-based cross-border investment firm described as focusing on “blockchain technology applications, game equipment leasing, online game technology research and development and project investment,” as well as investments in American electronic gambling equipment manufacturing and gambling game development.[196]

Beyond North America, similar partnerships have been observed expanding across Europe in recent years, particularly involving Chinese as well as Vietnamese money laundering networks who have helped launder hundreds of millions of Euros. Authorities have found these sums to have been generated by local criminal groups operating in countries including Albania, France, Germany, Ireland, Italy, Lithuania, Spain, UK, and elsewhere in Europe involved in the trafficking of narcotics and counterfeit goods, tax and customs

191 United States Immigration and Customs Enforcement, Department of Homeland Security Investigations, “HSI Chicago Investigation Lands Chinese National 10 Years in Prison for Laundering $62 Million in Drug Proceeds”, December 2024, available at: https://www.ice.gov/news/releases/hsi-chicago-investigation-lands-chinese-national-10-years-prison-laundering-62.

192 United States Attorney’s Office, Northern District of Illinois, “Suburban Chicago Man Sentenced to Seven Years in Federal Prison for Laundering Drug Trafficking Proceeds”, November 2022, available at: https://www.justice.gov/usao-ndil/pr/suburban-chicago-man-sentenced-seven-years-federal-prison-laundering-drug-trafficking#:~:text=In%20the%20summer%20and%20fall,proceeds%20in%20the%20United%20States.

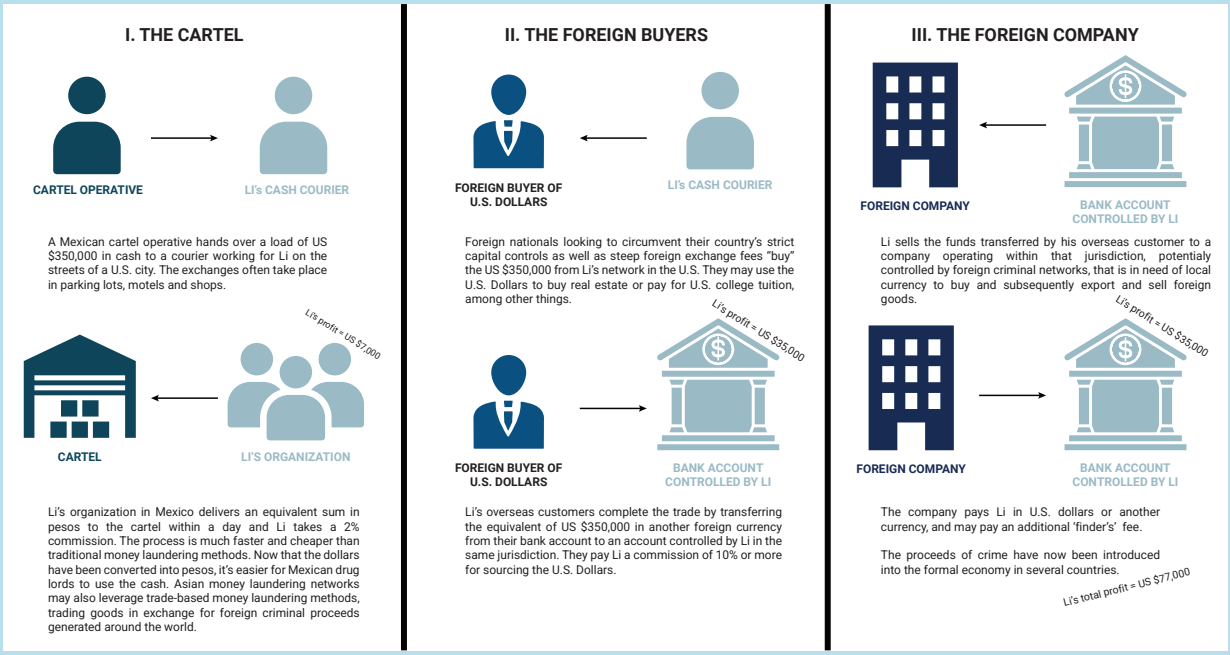
193 United States Attorney’s Office, Northern District of Illinois, “Chinese National Sentenced to Ten Years in Prison for Laundering $62 Million in Drug Proceeds on Behalf of Mexican Traffickers”, December 2024, available at: https://www.justice.gov/usao-ndil/pr/chinese-national-sentenced-ten-years-prison-laundering-62-million-drug-proceeds-behalf.

194 United States Department of Justice, Press Release, October, 2021, available at: https://www.justice.gov/archives/opa/pr/leader-money-laundering-network-responsible-laundering-millions-dollars-drug-proceeds.

195 United States District Court Southern District of New York, “Case 1:19-cv-01033”, 01 February 2019, available at: https://src.bna.com/FhO.

196 OTC Market, “Disclosure Statement Pursuant to the Pink Basic Disclosure Guidelines INVECH HOLDINGS IN”, 30 April 2019, available at: https://www.otcmarkets.com/financialReportViewer?symbol=IVHI&id=223360.

Figure 6. Simplified mirror transaction model used by the Xizhi Li Network



Elaboration based on United States Department of Justice and visualization by Propublica, 2022. Source: United States Department of Justice, 2021.

fraud, and prostitution.[197,198,199,200]

In recent years, international law enforcement has also reported a dramatic intensification of drug trafficking from South America to the Asia Pacific region, with this trend further indicating the possibility of a widening scope of collaboration between Asian and South American criminal groups beyond money laundering.[201] Taken together, these additional details highlight the growing financial integrity and international and regional security risks posed by the evolving partnerships and tactics increasingly characterizing market leading Asian MLOs.

197 European Public Prosecutor's Office, "Italy: EPPO uncovers Chinese underground banking network suspected of €113 million VAT fraud", 25 October 2024, available at: https://www.eppo.europa.eu/en/media/news/italy-eppo-uncovers-chinese-underground-banking-network-suspected-eu113-million-vat.

198 Europol, "French and Spanish authorities crack down on Chinese money laundering gang", July 2021, available at: https://www.europol.europa.eu/media-press/newsroom/news/french-and-spanish-authorities-crack-down-chinese-money-laundering-gang.

199 Institute for Financial Integrity, "Collaboration Between Chinese Money Laundering Organizations & Drug Cartels", 28 August 2024, available at: https://finintegrity.org/collaboration-between-chinese-money-laundering-organizations-drug-cartels/.

200 Europol, *French and Spanish authorities crack down on Chinese money laundering gang*.

201 UNODC, Synthetic Drugs in East and Southeast Asia, 2024.

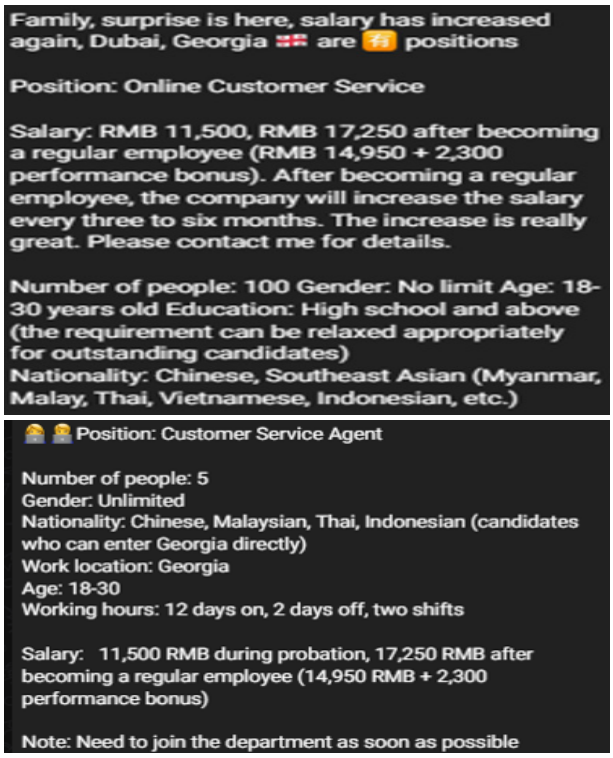
South Asia

South Asian nations have also come into the orbit of the regional online crime sphere. While India has long been a base for call centre scam operations, as the industry grew in Southeast Asia, it became both a target for scam operators and a source of labour. This is reflected in the large number of Indian nationals repatriated from Myawaddy compounds in March 2025 (see earlier), and successful efforts by the Indian Government to extract nationals from compounds in Lao PDR and Cambodia.[202] Raids and rescues have also identified Pakistanis, Bangladeshis and Nepalis from scam sites across the region. Sri Lanka has also emerged as a base of operations. In 2024, a number of raids led to the arrest of hundreds of people, including Chinese, Malaysian, Filipino, Thai, Vietnamese, and Indonesians, found at suspected cyber-enabled fraud operations, providing further evidence of expansion beyond Southeast Asia.[203] In a statement last year, the Chinese Embassy in Sri Lanka noted that law enforcement action in Myanmar, Cambodia, and the United Arab Emirates had significant results, but led to some criminal groups moving to countries peripheral to Southeast Asia.[204]

Georgia and Türkiye

Cyber-enabled fraud operations have established a strong foothold in Russia and several former Soviet republics. In March 2025, investigative reporting supported by official sources exposed a massive operation based in Tbilisi, Georgia, after internal files were leaked. The operation was found to have generated over US $35 million dollars from more than 6,000 victims since May 2022.[205] Although there is limited evidence to suggest the involvement of Asian criminal networks in this particular operation, there is evidence that East Asian crime groups have established a significant presence in Georgia in recent years, especially in the coastal city of Batumi.

Major East Asian crime groups have established bases in Batumi, as returned to in the second case study below. Online operations resembling those seen in Southeast Asia have been observed in Georgia, with multiple documented incidents of foreign nationals being detained and rescued reported in over the past year.[206] China's embassy in Georgia has recently also warned citizens about being deceived into illegal online work in the country.[207] Industry groups linked to Southeast Asian criminal networks on Telegram openly post recruitment ads for 'customer service' agents in Georgia. Many of these posts are in Chinese, and seek recruits from China and Southeast Asia who are fluent in Chinese.



Online recruitment ads for various positions in Georgia posted by vendors within various illicit online marketplaces in Southeast Asia, 2025.

Elsewhere in Europe, Türkiye has been cracking down on online gambling, cyber-enabled fraud operations and associated money laundering. Several law enforcement operations have targeted companies registered in Istanbul's Grand Bazar which have been used to launder illicit proceeds. Although information on involvement of East Asian actors is limited, it has been observed that several Chinese actors detained elsewhere for involvement in online crimes have been able to secure Turkish nationality. This notably includes Lin Baoying, one of the ten convicted in the Singapore money laundering case.

202 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, *p.48.*

203 Sri Lanka Police Service, "Official Media Statements", October 2024.

204 Embassy of the People's Republic of China in Sri Lanka, "Notices and Announcements", October 2024.

205 Organized Crime and Corruption Reporting Project, Scam Empire, March 2025.

206 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*.

207 Embassy of the People's Republic of China in Georgia, "Consular reminder on being highly vigilant against cross-border online gambling and telecommunications fraud", 8 May 2023, available at: https://ge.china-embassy.gov.cn/chn/lsfw/202110/t20211015_9544011.htm.

Targeting of the United Arab Emirates by Asian crime syndicates

The United Arab Emirates (UAE) have been targeted as a base for individuals involved in the laundering of funds acquired through illicit online activity, many of whom have purchased property in Dubai. In 2024, a dual national of China and Saint Kitts and Nevis pleaded guilty at court in the Central District of California to laundering over US $73 million in proceeds of cryptocurrency investment scams. Court documents identified him as being resident in Cambodia and UAE.[208]

As detailed in previous UNODC and official government reporting, so-called "OTC King", Zhao Dong, and several associates were also recently convicted by authorities in China for operating platforms that provided payment and settlement services to criminal groups involved in large-scale online gambling and cryptocurrency investment fraud in Southeast Asia. Prosecutors found that the platforms' laundering process involved conversion of Dirhams in Dubai into USDT and then back to Renminbi in China.[209] Official testimony and affidavits produced in court as well as other corporate and legal filings also show that several of those convicted in Singapore's 2023 SG $3 billion money laundering investigation held extensive property portfolios in Dubai.

In addition to considerable exposure to money laundering risks, there has been strong indication of criminal groups attempting to expand physical online fraud operations in the country. In 2024, this culminated in a rapid crackdown by UAE authorities targeting several clandestine online crime sites, reportedly leading to hundreds of arrests.[210] The operation caused significant disruption, however, regional law enforcement and other sources in East and Southeast Asia have indicated that the UAE remains an important base for these operations.[211]



Dubai authorities raid cyber-enabled fraud operations at the Rahaba Residence, April 2024. Source: Al Khaleej newspaper and Khaleej Times, 2024.

As detailed earlier, the UAE has been identified as a recruitment hub for people who have been rescued or detained working in Asian-led online operations.[212] Philippines authorities have warned overseas workers based there about recruitment traps, and identified a group of nationals arrested in Nigeria in 2024 as being recruited in Dubai.[213] Sri Lankan authorities have also warned nationals in Dubai after identifying an increase in people in the emirate being recruited to cyber-enabled fraud operations in Myanmar.[214] In recent years various sub-national public security bureaus in China have issued calls for residents involved in overseas online gambling and fraud to return to China and surrender. Many of these notices have explicitly mentioned the UAE alongside Myanmar, Lao PDR and Cambodia. China's Ministry of Public Security has also sent working groups to UAE for joint law enforcement activities.[215]

208 United States Department of Justice, "Foreign National Pleads Guilty to Laundering Millions in Proceeds from Cryptocurrency Investment Scams", 12 November 2024, available at: https://www.justice.gov/archives/opa/pr/foreign-national-pleads-guilty-laundering-millions-proceeds-cryptocurrency-investment-scams.

209 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape, p.76-77.*

210 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

211 Ibid.

212 Humanity Research Consultancy, "Uncovering the Spread of Human Trafficking for Online Fraud into Laos and Dubai", July 2024, available at: https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/66bec89de33fb0311442d888_Asia-CTIP%20Laos%20Dubai%20Investigation.pdf.

213 Department of Migrant Workers, "DMW warns OFWs vs 'third country recruitment'", 13 January 2025, available at: https://dmw.gov.ph/news-releases/2025/DMW-warns-OFWs-vs-third-country-recruitment.

214 National Anti-Human Trafficking Task Force, "NAHTTF issues a warning on the trafficking of Sri Lankans in the UAE to the cyber scam centres in Myanmar", 11 November 2024, available at: https://www.defence.lk/Article/view_article/28239.

215 Criminal Investigation Bureau of the Ministry of Public Security of the PR China, "268 suspects of cross-border telecommunications fraud were handed over to us", 28 February 2024, available at: https://mp.weixin.qq.com/s/MDwk9tyxeQcaz48NfvQzXw..

Law enforcement action in Isle of Man continues to target online gambling and transnational criminal actors

As covered in previous UNODC analysis,[216] organized crime groups have expanded into the Isle of Man, a jurisdiction that hosts numerous 'white label' companies that have received licenses to operate online casinos. In April 2024, Isle of Man constabulary raided the offices of a major online gaming company in connection to a wider fraud and money laundering investigation.[217] This led to the suspension and later cancellation of its licenses, as well as associated companies, including a virtual asset firm, which was ultimately deregistered.[218]

Examination of corporate filings and court documents shared by regional law enforcement authorities confirmed that, in 2023, a Chinese court convicted six people who worked for another affiliate company which operated from an initial base in the Philippines before being transferred to the Isle of Man, with the court finding that the syndicate defrauded victims in mainland China out of millions of dollars through fraudulent investment schemes.[219] The company's co-founder is also known to have developed strong connections to Lao PDR and sanctioned businessman and alleged crime boss, Zhao Wei, who chairs the Golden Triangle Special Economic Zone in recent years prior to his expansion into the Isle of Man.[220]

Further law enforcement action took place in March 2025, when police raided the offices of two companies, confirmed to be Ableton Prestige Global Limited and Amiga Entertainment Limited, arresting two people. The raids were described by Isle of Man authorities as part of "a large-scale international money laundering investigation," with corporate filings indicating both companies to be owned by a criminally implicated business group active in Cambodia that has been extensively linked to illegal online gambling and cyber-enabled fraud.[221,222]

216 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, p.31-32.

217 Isle of Man Constabulary spokesman "Seven arrests in 'series' of police raids linked to Isle of Man gaming company investigation", Isle of Man Today, 29 April 2024, available at: https://www.iomtoday.co.im/news/seven-arrests-in-seriesof-police-raids-linked-to-isle-of-man-gaming-companyinvestigation-683322.

218 Isle of Man Gambling Supervision Commission, "Public Statement Suspension of Gambling Licences", April 2024; Isle of Man Gambling Supervision Commission, "Public Statement: Cancellation of Gambling Licence for Dalmine Limited", 24 July 2024, available at: https://www.isleofmangsc.com/ gambling/news-gambling/24-july-2024-public-statementcancellation-of-gambling-licence-for-dalmine-limited/; Isle of Man Gambling Supervision Commission, "Public Statement: Cancellation of Gambling Licence", July 2024; Isle of Man Financial Services Authority, "Soteria Solutions Limited – issue of direction", April 2024; Isle of Man Financial Services Authority, May 2024.

219 Wuzhi County People's Court of Henan Province, Criminal Judgement, "Case No. 579", 2023.

220 Golden Triangle Special Economic Zone Administration, "Official media release", December 2018.

221 Isle of Man Constabulary statement, 13 March 2025.

222 UNODC, Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape,

Corruption as a key enabler

Corruption remains a critical enabler and facilitator for organized crime groups in East and Southeast Asia, and beyond. Legislative and regulatory gaps in anti-corruption frameworks have allowed corrupt behaviours to persist, creating exploitable loopholes for criminal actors with little consequence. Such gaps in the private sector have remained prevalent in Southeast Asia, where corrupt acts have not yet been adequately criminalized. For example, six of 10 ASEAN Member States[223] have yet to criminalize bribery in the private sector or only have laws which are narrow in scope – such as laws which only apply where private individuals have conspired with public officials. Additionally, as criminal actors seek to rely on complex corporate structures and shell companies to evade liability, legal frameworks to detect, investigate, and prosecute corrupt behaviour committed by legal persons remain lacking. Significantly, eight out of

223 UNODC, "Implementation of chapter III: Criminalization and law enforcement in ASEAN States parties and Timor-Leste," 2024, p. 24, available at: ttps://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_of_UNCAC_Chapter_III_-_ASEAN_States_parties_and_Timor-Leste_March_2024_updated.pdf.

ten ASEAN Member States[224] have not adequately provided for the liability of legal persons, with some domestic systems unable to fully recognize legal persons as actors of crime. Out of the eight, seven lack sanctions for legal persons that are effective, proportionate and dissuasive. In the absence of legal certainty and deterrence, criminal actors and organized crime groups remain incentivized to exploit corporate structures for illicit purposes.

Preventing corrupt behaviour and strengthening safeguards in the private sector remain fundamental in disincentivizing the operation of criminal networks, who may seek to masquerade as legitimate business ventures or foreign investors. In particular, beneficial ownership transparency can be a key tool in preventing the misuse of corporate vehicles to conceal the proceeds of corruption and other illicit gains.[225] However, the majority of ASEAN Member States[226] have yet to implement adequate measures to ensure the transparency of legal persons and arrangements, including clear mechanisms to verify, share, and maintain up-to-date information on beneficial owners. The lack of such critical mechanisms allow criminals to exploit fraudulent identities, proxies, or avail the services of intermediaries – brokers, professional service companies, and lawyers – to maintain the secrecy of their identity.

Individuals and often victims who seek to report corrupt behaviour face significant risks in doing so. They may face retaliation inside and outside of the workplace, including the potential threat of physical harm, and may, where relevant, face exacerbated dangers as foreign nationals or migrant workers. Despite the important role played by whistle-blowers in detecting and preventing of corruption and other forms of wrongdoing, legislation and frameworks to protect them continue to remain underdeveloped. In Southeast Asia, only three out of 10 ASEAN Member States[227] have enacted dedicated whistle-blower protection legislation – and even with such legislation, potential limitations remain in the scope of protective measures and persons covered. For example, whistle-blowers reporting on misconduct in the private sector may not be able to be protected. Other practical barriers can deter individuals to report on wrongdoing, such as insufficient disclosure channels and a lack of anonymous reporting. Moreover, while witnesses were generally acknowledged as a category of persons requiring protection, such comprehensive protection was not always available in Southeast Asia – in particular, nine out of ten ASEAN Member States[228] were deemed to have legislative and regulatory in the provision of safety measures, with many lacking resources and adequate witness protection programmes.

The insufficient criminalization of obstruction of justice in Southeast Asia further exacerbates these challenges. Obstruction of justice can involve the use of inducement, threats or force to interfere with witnesses and officials, whose role would be to produce accurate evidence and testimony. Five ASEAN Member States[229] were deemed to have only partially criminalized obstruction of justice, leaving gaps which criminal actors may seek to exploit. For example, while using physical force to interfere with a law enforcement official's duty was commonly criminalized, attempts to interfere with witnesses or the production of evidence may not be.

Together, these legislative and regulatory gaps can create an environment where serious criminal wrongdoing is enabled and facilitated by corruption. Failures to detect, investigate, and prosecute individual corrupt acts can lead to systemic gaps which are exploited by organized criminal groups.

Implications for the region and beyond

Cyber-enabled fraud and illegal online gambling has taken root in Asia, eroding institutional integrity and benefiting from and fueling corruption. The impacts of this are observed in countries hosting online operations, but also countries where supporting infrastructure is located, those that act as trafficking routes, locations where transnational crime actors hide proceeds and acquire property, and those that have provided citizenship to criminal actors. While the impacts of the industry are global,

224 Ibid, p. 29.

225 UNODC, "Implementation of beneficial ownership transparency in ASEAN Member States and Timor-Leste," 2024, p. 3, available at: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_of_Beneficial_Ownership_Transparency_in_ASEAN_Member_States_and_Timor-Leste.pdf.

226 Ibid.

227 UNODC, "Whistle-blower protection in ASEAN Member States," 2023, p. 4, available at: https://www.unodc.org/roseap/uploads/documents/Publications/2023/Whistlerblower_Protection_in_ASEAN_-_2023_UNODC_paper.pdf.

228 UNODC, *Implementation of chapter III : Criminalization and law enforcement in ASEAN States parties and Timor-Leste*, p. 40.

229 Ibid, p. 28.

it has unique and serious impacts at the country-level across multiple jurisdictions.

Although relative normalcy has returned after the upheaval caused by the COVID-19 pandemic, its economic impacts are still being felt. One industry that suffered catastrophic consequences in Southeast Asia was tourism. Following the onset of the pandemic and through the periods of lockdown, international arrivals dropped to almost nothing. During this time, thousands of businesses shutdown, destroying livelihoods and depriving countries of crucial tax revenues. Impacts were felt from family businesses up to major hospitality companies and airlines.

Countries like Cambodia and Thailand have gone through the painful process of rebuilding their tourism industries and bringing tourists back. Yet, the persistence of scam operations in the region and the resulting reputational damage has likely undermined these efforts, especially among the Chinese population, which over the past decade have become a mainstay of their tourism sectors. This came to the fore in Thailand in early 2025 when the Chinese actor Wang Xing was trafficked from Thailand to Myanmar and held in a border scam compound.[230] Following intense coverage of the case, numerous reports indicated that Chinese tourists had cancelled trips to Thailand.[231] Although this is a single case, there are many like it, and as these issues persist the reputational harm and negative risk perception of the global public continues to increase.

Beyond the tourism industry, the spread of organized criminal activity in Southeast Asia has implications for legitimate business, investment and trade. Again, deepening reputational problems could dissuade potential investors from establishing operations in certain countries, or dampen established companies' willingness to expand. Scam operations, illegal online gambling, casinos and the various criminal activities that emanate from and revolve around them also bring increased rates of crime, raising legitimate security concerns among the licit business community.[232]

This potentially raises the cost of doing business, with companies having to increase expenditure on security, and insurance premiums and loan interest rates likely rising to reflect risk factors. The endurance and expansion of criminal activity in the region therefore jeopardizes the ongoing work of countries to strengthen their economies in the post-pandemic period.

The context in Myanmar is unique in that it is currently in the depths of conflict since the military takeover in 2021. The economic and social impacts have been extensive, and as the country has once again become deeply isolated from the international community and the global economy, both incomes and employment opportunities have plummeted. With limited options available, Myanmar youth have begun to migrate to work in online operations in border areas, and the country must now reckon with a generation of young people being drawn into criminal activity.[233] There are also increasing signs of Myanmar nationals being found in scam operations in other countries in the region, with some syndicates documented recruiting vulnerable internally displaced people (IDPs).[234] More than this, revenues derived from scam centers are likely exacerbating the conflict by being distributed among various actors offering protection and support to criminal operations in non-state armed group-controlled regions and other areas.

The persistence of the industry also has profound regional impacts. First and foremost, there is potential for the ongoing situation to put a strain on bilateral relations, in turn creating tensions within ASEAN. While the industry is transnational, and there are culpable actors across the region, a handful of countries are hosting the bulk of operations, which are targeting the citizens of neighbouring countries. Drastic actions such as those taken by Thailand in February this year can also potentially alienate law abiding populations in border areas who are impacted by measures such as energy and fuel cuts.

Online gambling and cyber-enabled fraud also have the potential to worsen pre-existing security and

230 Royal Thai Police, "Stakeholder Roundtable Closed-Door Meeting", Bangkok, Thailand, February 2024.

231 Travel agents in both Thailand and China expressed concerns that a significant drop in tourists was likely, and Chinese social media was flooded with messages by people saying they had cancelled planned trips.

232 For example, there have been alarming reports of kidnapping for ransom of businesspeople in the region, with perpetrators often linked to organised crime.

233 Concerns shared by various civil society groups in discussion with UNODC, also reflected in media reporting that has interviewed Myanmar nationals that work or have worked in illegal gambling and scam operations.

234 Official law enforcement reporting and discussions with anti-trafficking groups have identified Myanmar nationals rescued or arrested in Thailand, Cambodia, Laos and the Philippines, while IDPs have also been rescued in the region.

conflict risks. The now industrialised trafficking networks spread across the region take advantage of porous borders, and a distinct sub-industry of actors involved in facilitating transport and illegal border crossings has developed. This has implications for other crimes, including trafficking in persons for other purposes, smuggling of migrants, and the movement of narcotics and arms. The intersection with armed groups, especially in Myanmar, also risks exacerbating conflict, which is disastrous for local populations and can also have spillover effects on neighbouring countries.

The global implications have been illustrated in the mass of reporting on cases where people have fallen victim to cyber-enabled fraud. In East and Southeast Asia alone, UNODC estimates that cyber-enabled fraud caused financial losses between US $18 billion and US $37 billion in 2023, the majority attributed to scams committed by organized crime groups in Southeast Asia.[235,236]

Across the world, reported losses caused by cyber-enabled fraud have increased exponentially. For example, fraud is now the most commonly recorded crime in England and Wales, although only a fraction of cases are likely to be reported. According to the National Crime Agency, in 2024 romance and investment fraud had increased significantly, and 89% of reported fraud is now cyber-enabled, with the majority committed entirely or partially from overseas.[237] In Australia, the National Anti-Scam Centre reported recorded losses of over AU $2 billion in 2024.[238] Many of these scams can be traced to the region, and in November 2024, Philippines law enforcement worked with Australian Federal Police to examine equipment seized during a raid on a scam operation in Pasay. Officers were able to identify over 5,000 Australians who had been contacted by the scammers from this one operation.[239]



Australian and Philippines law enforcement agencies cooperate to bring down and investigate scam operation located in Pasay City. Source: PAOCC and AFP.

It is also worth noting that cyber-enabled fraud and illegal online gambling have a broader corrupting impact on the societies and systems that they integrate with. Large-scale online crime operations could not exist without official complicity of some type, be that border enforcement who allow workers and trafficking victims to cross without hindrance,

235 The total estimated financial loss is the sum of the losses from cyber-enabled fraud victims across 12 countries and territories in East and Southeast Asia: China, Hong Kong (China), Macau (China), Indonesia, Japan, Malaysia, the Philippines, the Republic of Korea, Singapore, Thailand, Taiwan Province of China, and Viet Nam. For each country and territory, the estimated financial loss was calculated using the following formula: Estimated financial loss per country = (Reported financial loss) × (100 ÷ Reporting rate (%)).

236 Another approach to understanding the size of the cyber-enabled fraud industry in Southeast Asia is by examining the proceeds generated by people working within it. Based on information provided by regional law enforcement agencies, UNODC estimates that organized criminal networks engaged in cyber-enabled fraud generate between US $27.4 and $36.5 billion annually. This range is based on the estimated labour force in scam centres in 10 Southeast Asian countries (ASEAN members) and the average amount of proceeds generated (or stolen) by each individual. While this estimate offers a different perspective and also highlights the sheer scale of the industry in Southeast Asia, there are uncertainties regarding both estimated labour force and average revenues generated per person.

237 National Crime Agency, "National Strategic Assessment of Organised Crime", 2024. available at: https://www.nationalcrimeagency.gov.uk/threats/nsa-fraud-2024.

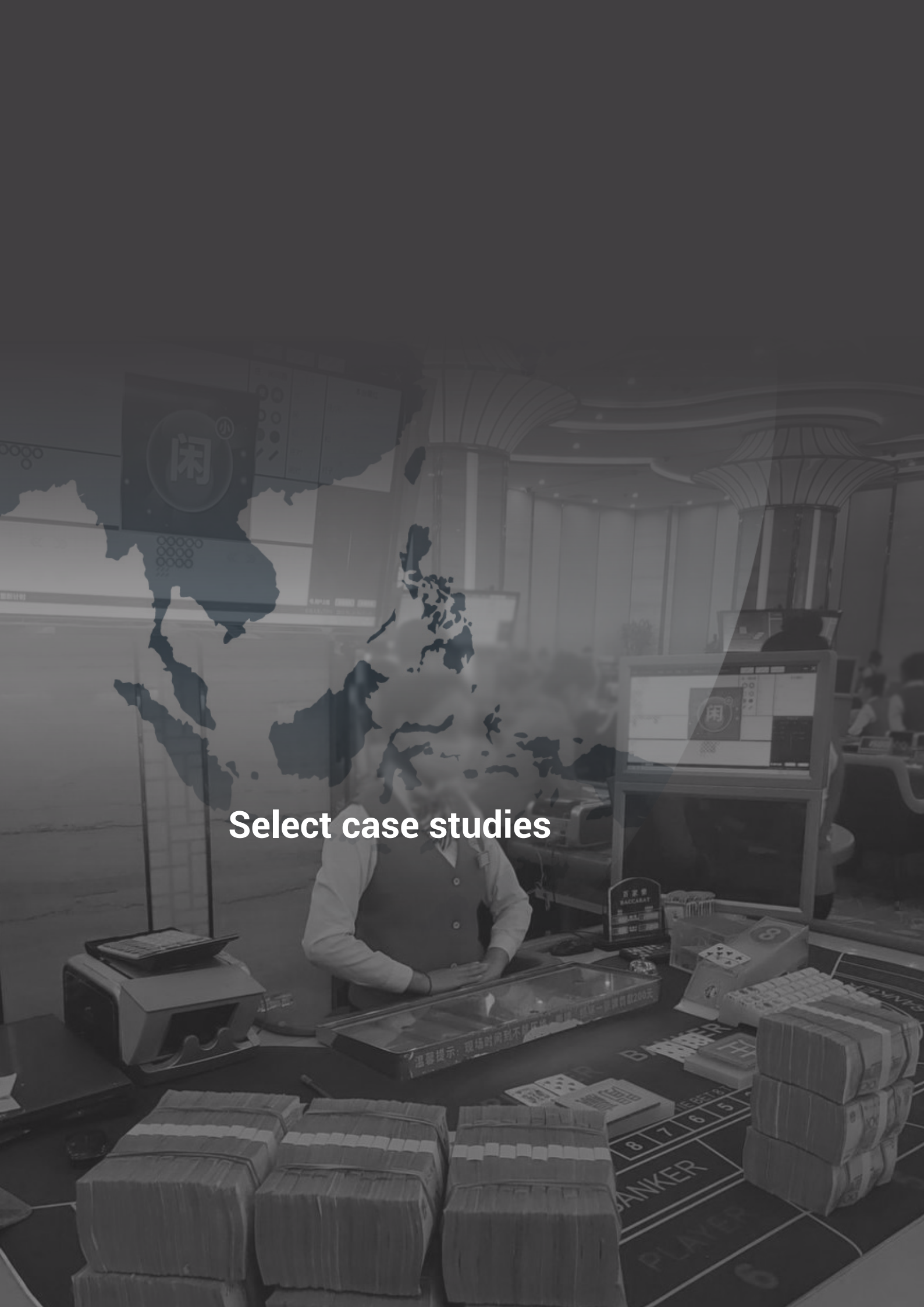
238 National Anti-Scam Centre, "Targeting Scams: Report of the National Anti-Scam Centre on scams data and activity", 2024, available at: https://www.scamwatch.gov.au/system/files/targeting-scams-report-2024.pdf.

239 AFP, National Anti-Scam Centre, Philippines Presidential Anti-Organized Crime Commission and National Bureau of Investigation, "More than 5000 Australian victims receive text warning over romance scam", 31 January 2025, available at: https://www.afp.gov.au/news-centre/media-release/more-5000-australian-victims-receive-text-warning-over-romance-scam.

or local police and regulators that fail to identify, inspect, and shut down the operations that are often operating out in the open. Gambling and fraud transactions have resulted in massive unregulated capital outflows from the countries targeted, and at the other end, the criminal actors behind these operations have channeled proceeds of crime into global financial systems, including digital currency platforms and traditional banks, while using them to acquire assets including property in financial hubs such as London, Singapore and Dubai.

Lastly, the growing global impact of expanding Asian money laundering and underground banking networks cannot be understated. As examined in an earlier section, governments from around the world have reported accelerating collaboration, partnerships, and synergies forming between globalized criminal networks centred in Southeast Asia and major criminal groups based elsewhere around the globe. Moreover, many of the region's largest criminal groups have shifted towards the development of key infrastructure and infiltration of legitimate financial industries - particularly those related to online payment processing, blockchain technology, and cryptocurrency trading and exchange services. There is also growing indication of targeting of compliance-related businesses involved in platform on-boarding and customer due diligence and KYC processes, leading to concerns of further infiltration of the virtual asset ecosystem.

The impact of this shift has proven highly consequential for countries both within and beyond Southeast Asia, enabling transnational organized crime to scale up illicit activities by dramatically reducing the cost of money laundering and improving the speed, efficiency, and anonymity with which it can take place. More than this, as these mutually beneficial relationships continue to evolve and progress, they pose significant risks of galvanizing transnational organized crime in other regions – many of which are emerging as important nodes within underground networks and ecosystems being advanced by Asian crime syndicates.



Select case studies



Tip of the iceberg: Updates involving Singapore's multi-billion-dollar money laundering case

In August 2023, authorities in Singapore announced the country's largest ever money laundering investigation, culminating in the arrest and conviction of 10 foreign nationals suspected of laundering the proceeds of overseas organized crime activities, including illegal online gambling and telecommunication scams. Singapore police conducted a series of sweeping raids across the city-state, consisting of more than 400 officers initially seizing close to SG $1 billion (US $732 million) in cash and Tether (USDT), real estate, luxury cars, other assets including over 250 luxury handbags, jewelry, and watches.[1] The 10 suspects were convicted on various charges and sentenced to between fifteen and eighteen months imprisonment.[2]



Seized assets and bulk-cash reported during the Singapore raid. Source: Singapore Police Force, 2023.

In what followed, the value of seized assets increased to approximately SG $3 billion (US $2.3 billion), with all of those arrested pleading guilty to various financial crimes, including efforts to obscure the source of their funds. This included submitting forged property sales contracts, loan documents, bank and corporate financial statements, producing false income certificates, and utilizing unregulated and illegal online gambling platforms. Moreover, beyond Singapore, the group collectively owned or had documented links to dozens of companies, held bank accounts, and high-value real estate in countries including Cambodia, China, Hong Kong, China, Cyprus, the Philippines, Thailand, UAE, the United Kingdom, and Jersey.[3] While all were originally from Fujian, China, they acquired additional citizenships from countries including Cambodia, Cyprus, Dominica, Saint Kitts and Nevis, Saint Lucia, Türkiye, and Vanuatu. Nine held Cambodian citizenship, and several held multiple passports, with one individual having held citizenship for five different countries.[4] At least 17 others remained under investigation, with several fleeing the country before or after the raids.[5]

1 Singapore Police Force, "Ten Foreign Nationals To Be Charged For Offences Including Forgery And Money Laundering With An Estimated Value Of About One Billion In Cash And Various Assets Seized, Frozen Or Issued With Prohibition Of Disposal Orders", 16 August 2023, available at: https://www.police.gov.sg/Media-Room/News/20230816_10_Foreign_Nationals_Offences_Forgery_Money_Launder_Est_1_Bil_Assets.

2 Ibid.

3 As per corporate records reviewed by UNODC and affidavits presented before the court and captured in trial reporting.

4 Although all were born in China, police reports describe only three as Chinese, while the others were recorded as Cambodian, Cypriot, Turkish, Vanuatuan. Documents reviewed by UNODC and affidavits presented during the trial revealed all held multiple nationalities.

5 UNODC, *Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud*, August 2024.

Although the full extent and exact sources of their wealth is not known, charges largely focused on laundering of funds acquired through illegal online gambling activities, specifically in the Philippines, despite indication of the group's broader criminal footprint in Southeast Asia.[6] However, experts agree that this complex web of interlinked companies, shells, fraud, illegal online gambling, and cryptocurrency trading platforms is consistent with new and evolving modus operandi attributed to criminal networks based in Southeast Asia, increasingly impeding financial investigations, criminal justice, and financial integrity globally.

In the months following the initial investigation by Singaporean authorities, information has continued to surface highlighting links between those convicted and numerous confirmed scam centres in Cambodia and the Philippines targeting European and North American victims, as well as a collapsed cryptocurrency trading platform in Hong Kong, China which defrauded hundreds of investors, with losses totaling more than US $30 million.[7,8,9,10,11] This includes direct connections to multiple dismantled cyber-enabled fraud operations involving the Sun Valley Clark Hub, Baofu Land Development Co., Zun Yuan Technology, and Hong Sheng Gaming Technology, alongside other companies and assets registered in Singapore, Cambodia, China, including Hong Kong and Taiwan PoC, Cyprus, Seychelles, Turkey, UAE, Canada, and elsewhere. Moreover, this includes links to the Atom Asset Exchange (AAX), a major criminally implicated Hong Kong-based cryptocurrency exchange that collapsed in 2022, leading to the arrest of a senior executive in 2024.

As shown in figure 1, examination of corporate documents confirms that Wang Shuiming and Associate 1, who were respectively convicted and identified as a main suspect (now fugitive) in the Singapore money laundering case, were connected to AAX Director and alleged shadow Chief Executive, Associate 2, through two financial and technology companies incorporated in Xiamen, China and Taiwan PoC as joint shareholders holding senior positions. Associate 2, who was arrested in July 2024 by authorities in Hong Kong, China, is also listed as an owner of two Hong Kong companies with the co-founder of the Philippines' Sun Valley Clark Hub, where police rescued more than 1,000 trafficking victims in 2023.[12,13] Victims were forced to target foreign nationals from Canada, the United States, and across Europe to invest in fraudulent cryptocurrency investment platforms.[14]

According to experts, the shared companies could also signal a mix of legitimate and illicit business interests and financial flows, with one possible risk being the use of stolen funds to capitalize and provide liquidity to a major licensed cryptocurrency exchange established and controlled by organized crime. Additionally, it is worth noting that corporate records examined by UNODC confirm connections between Wang Shuiming and a senior member of the Sun Ye On Triad, while other recent legal filings indicate that significant amounts of the stolen AAX assets controlled by Associate 2 and his wife, a Canadian national, may have been moved to Canada prior to the arrest.[15,16]

Further demonstrating this network's connections to broader regional crime groups, individuals involved in the AAX exchange have direct connections to one criminally-implicated Mekong-based conglomerate. The entity possesses well-documented links to several large compounds hosting online gambling and cyber-enabled fraud operations, where cases of trafficking in persons for forced criminality have been reported. One of these sites, a casino in Bavet, Cambodia, was subject to sanctions by the United Kingdom in 2023.[17]

6 According to Singapore Police Force press releases following verdict of each of the ten defendants, published 2 April – 10 June 2024. For example, see: Singapore Police Force, "Tenth Person Sentenced For Forgery And Money Laundering Offences In Anti-Money Laundering Operation", 10 June 2024, available at https://www.police.gov. sg/media-room/news/20240610_ tenth_person_sentenced_ for_forgery_and_money_laundering_ offences.

7 UNODC, *Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud*, August 2024.

8 UNODC, "Closed-Door Roundtable on Cyber-Enabled Fraud and Transnational Organized Crime", Jakarta, December 2024.

9 Lancang-Mekong Integrated Law Enforcement and Security Cooperation Centre, "Closed-Door Information Sharing Meeting", February 2025.

10 Hong Kong Police Force, Official Press Conference and Case Briefing, July 2024.

11 UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*.

12 Philippine National Police, Media Release, May 2023.

13 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024

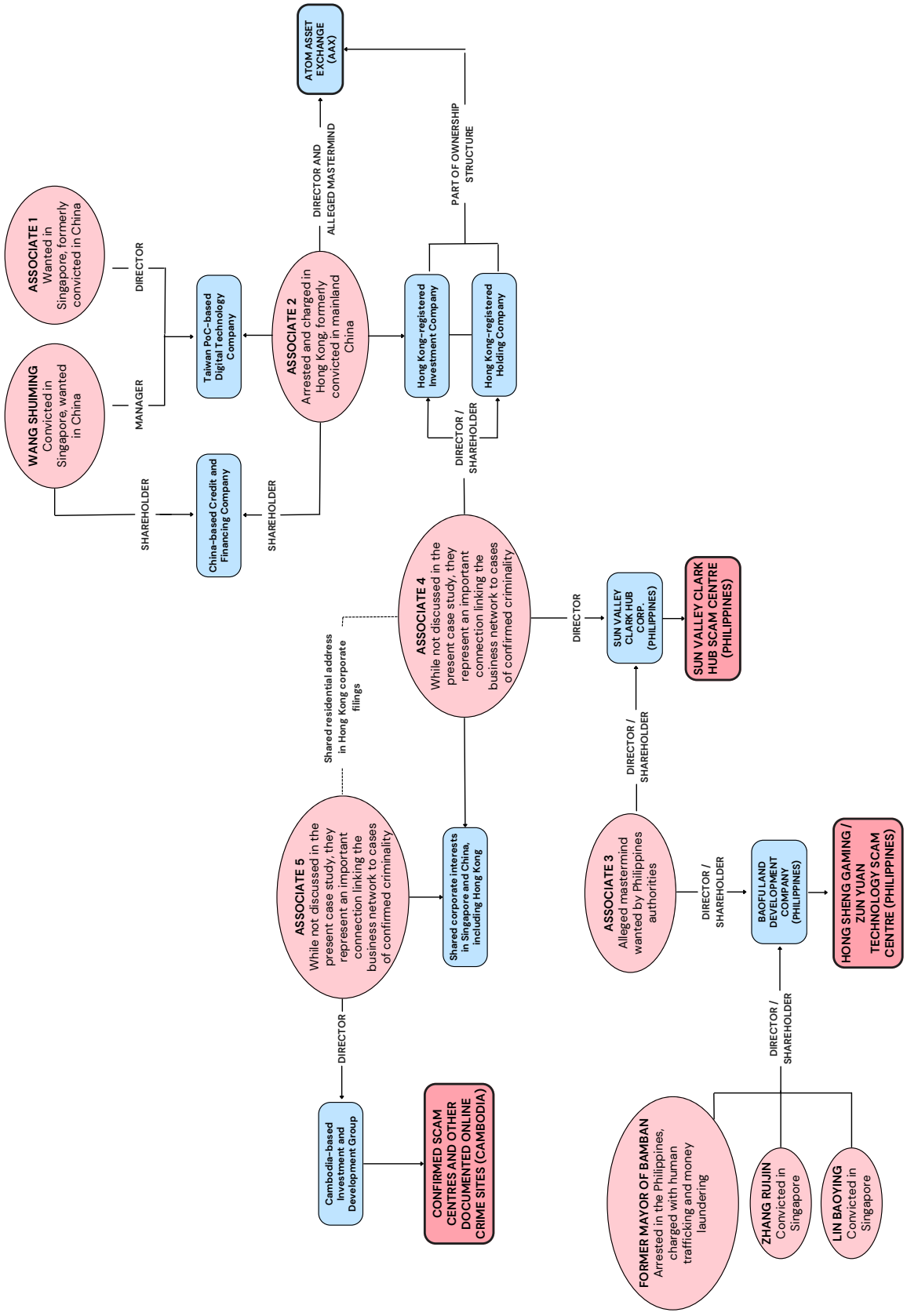
14 UNODC, Closed-Door Stakeholder Meeting on Cyber-Enabled Fraud and Transnational Organized Crime, Manila, Philippines, November 2024.

15 Examination of Related Hong Kong Corporate Filings, Companies Registry of Hong Kong, March 2025.

16 UNODC, Closed-Door Stakeholder Meeting on Cyber-Enabled Fraud and Transnational Organized Crime, Manila, Philippines, November 2024.

17 UK Government, "UK and allies sanction human rights abusers", 8 December 2023, available at: https://www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers.

Figure 1. Simplified network chart involving select suspects implicated in the Singapore money laundering case and elsewhere



Source: Elaboration based on UNODC examinations of multiple official sources.

Zhang Ruijin and Lin Baoying, two others convicted of money laundering and forgery in the Singapore case, were subsequently charged with trafficking in persons by Philippine authorities in September 2024 in connection to a major criminal investigation into the Baofu scam compound in Bamban, Tarlac, which was raided in March of that year. Police reported the rescue of over 800 individuals from China, the Philippines, Malaysia, Indonesia, Viet Nam, Rwanda, and Taiwan PoC at the site owned by Baofu Land Development, which was incorporated by five individuals including Zhang, Lin, and the former Mayor of Bamban. Authorities also charged the Mayor's fugitive business partner, Associate 3, who co-founded Baofu Land Development as well as Hong Sheng Gaming Technology and Zun Yuan Technology, which both held online gambling licenses at the time of their respective raids. While this individual managed to evade arrest and exit the Philippines, it is worth noting that he was also listed as a co-founder of the abovementioned Sun Valley Clark Hub Corporation, alongside another business partner of AAX director, Associate 2.



Aerial footage of the Baofu compound. Source: Inquirer.net 2024.

According to a legal petition submitted by the Philippines Anti Money Laundering Council (AMLC), Associate 3 operated in the country as a wanted fugitive in his native China, using a Cypriot passport and identity to set up companies and avoid detection. Notably, authorities further found that Associate 3 was able to escape the Baofu compound using the Mayor's personal helicopter.[18] His successful evasion of law enforcement has likely been aided by the fact that he holds multiple citizenships. Documents shared by PAOCC show he holds passports for China, Taiwan PoC, Cyprus, and Saint Kitts and Nevis. Cambodian naturalization decree records further show he also acquired Cambodian citizenship.

Taken together, these developments help provide a more detailed understanding of the level of sophistication, power, and access held by major Asian crime syndicates operating in Southeast Asia today, and how the opaque nature of their legitimate and illicit activities makes them so difficult to detect and disrupt.

18 UNODC, Closed-Door Stakeholder Meeting on Cyber Enabled Fraud and Transnational Organized Crime, Manila, Philippines, November 2024.



Convergence of organized crime: Examining a major Mekong-based criminal enterprise

The case of Business Group 2 (BG 2) provides a strong example of the sophisticated fronts and business structures developed by a major transnational criminal network operating globally yet centred in Southeast Asia.

Originating in Taiwan PoC but operating from a base in one Mekong country over the past decade, BG 2 has rapidly established itself as a major property developer with a public facing brand providing a front for an expansive portfolio of interests in land-based and online gambling, cyber-enabled fraud operations, and large-scale drug trafficking according to law enforcement sources.[1] Although the group now maintains a limited public footprint in Taiwan PoC, it rapidly become one of the most prominent foreign-owned conglomerates in the Mekong, with its diversified portfolio including casinos, hotels, real estate, restaurants, software development, biotechnology, logistics, trading, and media.

Led by two foreign born individuals from Taiwan PoC prior to their naturalization in multiple Southeast Asian countries, BG 2 has been observed developing strong connections with local elites through which they have been able to acquire large amounts of land, casino and online gambling licenses, and develop several high-profile real estate projects. More particularly, the Group owns a major online gambling brand and business-to-business software solution or white label, providing iGaming services to hundreds of licensed and unlicensed online gambling websites across the region and beyond. It also owns a land-based casino and has invested in a large business park located in one of the region's largest online gambling and cyber-enabled fraud hubs. This location has been the subject of multiple raids that have resulted in rescues of people claiming to be detained there and forced to engage in online crimes. Arrests have been made during these raids, during which undocumented foreign workers were found and a number of weapons and a small amount of drugs were seized.[2,3] One senior BG 2 executive is notably named in Taiwan PoC court documents in connection with large-scale methamphetamine production and trafficking and remains listed on Taiwan PoC's wanted list.[4]



A criminally implicated compound controlled by BG 2 in one Mekong country that has been extensively documented housing online gambling and cyber-enabled fraud operations, 2024.

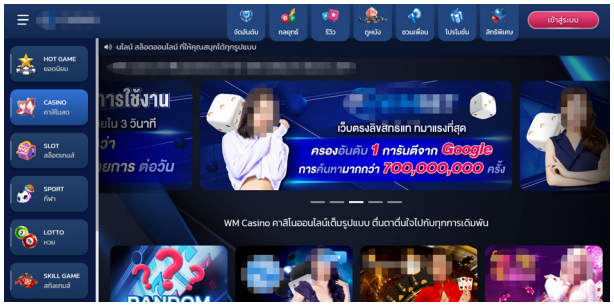
1 UNODC, *Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud*.

2 Provincial Police of One Mekong Country, Media Release, August 2022.

3 Based on consultations with several civil society and nonprofit organizations working to support victims of trafficking for forced criminality in the Mekong Region.

4 As per case documents available on Taiwan PoC Judicial Judgement Retrieval System and High Prosecutor's Office of Taiwan PoC Wanted Inquiry System.

In 2020, BG 2's now-dissolved Taiwan PoC-based online gambling and cloud technology company was named in a criminal court judgement regarding illegal gambling and related money laundering in which one defendant was sentenced to three years in jail.[5] Later in 2023, four employees of another associated company pleaded guilty to similar offences,[6] with court documents indicating that the company had handled services and transactions related to various BG 2-controlled online gambling platforms, many of which were further implicated in court judgements relating to large-scale money laundering and fraud offences between 2022 to 2024.[7]



Screen capture of BG 2's online gambling platform and white label software solution.

In addition to these operations, BG 2 also previously held interests in a casino boat located off the shore of Sihanoukville, Cambodia. This was jointly invested in by casino and junket operator, Jimei Group. The company, which was previously a major player in the Philippines casino sector, had its operations raided in 2016, with authorities arresting over 1,300 Chinese nationals for engaging in illegal online operations and various undocumented migration and labour violations. After allegedly trying to bribe officials following the raid, the company's chief executive fled the country and an arrest warrant was issued.[8]

More than this, BG 2 has been extensively linked to the criminally implicated Goddess of Liberty Group mentioned in previous sections of this report, establishing a joint venture in 2019.[9] The company was chaired by a senior BG 2 executive from Taiwan PoC who was arrested with other Goddess of Liberty executives including Liu Dawei in Uganda in 2021.[10] Although now dissolved, the joint venture company began to acquire property in Sihanoukville, Cambodia soon after it was formed, with its casino located directly adjacent to one owned and operated by BG 2. Solidifying these connections further, in 2020, Goddess of Liberty announced a major 6.7 hectare casino complex in Myawaddy, Myanmar, stating that the zone would be managed by BG 2.[11] However, the current status and ownership of the project is unclear at the time of writing following the arrest of Liu Dawei and other associates involved.

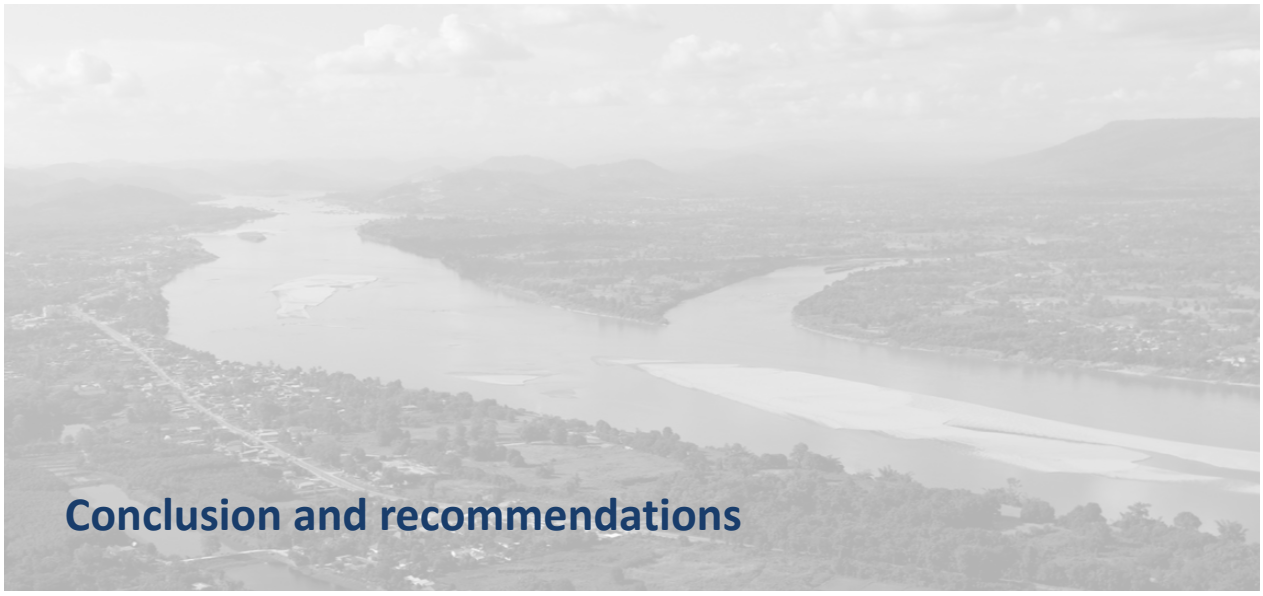
Beyond its deep engagement in Southeast Asia, BG 2 has also significantly expanded to Georgia, where the Group has registered at least 25 companies, including those holding properties and businesses connected to reports of cyber-enabled fraud.[12,13] Its interests are focused in the coastal city of Batumi, which has been increasingly associated with online gambling and cyber-enabled fraud operations similar to those documented in Southeast Asia. In recent years, BG 2 has also invested millions of dollars to become the main sponsor of a topflight Georgian football club, demonstrating its sustained effort to expand its legitimate public-facing brand and influence within the country.

Concerningly, dozens of active recruitment posts can be found online seeking Chinese and various Southeast Asian nationals to fill interpreter, assistant, and business development roles in Batumi on behalf of BG 2's Georgian-registered companies. Job descriptions are extremely vague, offering fully covered visa and travel expenses and dormitory accommodations, consistent with recruitment schemes used to deceive unsuspecting workers into cyber-enabled fraud operations in Southeast Asia.

5 Taiwan PoC Judicial Judgement Retrieval System.
6 Taiwan PoC Judicial Judgement Retrieval System.
7 Taiwan PoC Judicial Judgement Retrieval System.
8 UNODC, Closed-Door Stakeholder Meeting on Cyber-Enabled Fraud and Transnational Organized Crime, Manila, Philippines, November 2024.
9 Cambodian Ministry of Commerce Business Registry.
10 Uganda Police Force, Official Media Release, December 2021.
11 Goddess of Liberty, "Press Release: Myawaddy Goddess of Liberty Casino Goes Global", 1 February 2020, available at: https://www.tnaot.com/km/m/detail/article/9024154.
12 Corporate Filings Retrieved from Georgian Business Registry, March 2025.
13 UNODC, Regional Meeting of Analysts and Investigators on Transnational Organized Crime and Cyber-Enabled Fraud, Bangkok, Thailand, August 2024.

Conclusion and recommendations





Conclusion and recommendations

Transnational organized crime in Southeast Asia is evolving at a rate the region has never seen before. Driven by new service-based business models and technologies, rapid professionalization, and the ability to launder profits and shift value across borders undetected with unmatched speed and efficiency, Asian crime syndicates have not only managed to expand into new global markets, but have fundamentally taken hold of entire ecosystems they have built and infiltrated.

While the international community now stands at a critical inflection point amidst the accelerating linkages to Asian underground banking and money laundering networks and potential spin-offs of the regional scam industry, governments around the world are slowly coming to grasp the profound implications of the present situation. Taken together, it is increasingly clear that failure to address it will have unprecedented and potentially irreversible consequences for Southeast Asia that will be felt globally for years to come.

The following recommendations are intended to support countries in Southeast Asia in addressing the key vulnerabilities identified in this report, and ultimately to strengthen the awareness, understanding, and capacity of governments, oversight authorities, and law enforcement in Southeast Asia, and particularly those in the Mekong region. They build on targeted recommendations informed by ongoing dialogues and consultations with governments and law enforcement in the region, and are aligned with comprehensive and strategic recommendations agreed under the *ASEAN + China Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia*.[1]

Each priority area set out below addresses a distinct dimension of the response, while reinforcing the others. This approach is designed to be modular and scalable, enabling countries to adapt interventions to their specific national context while contributing to a unified and coordinated regional strategy.

Raising political awareness and will

Sustained political commitment is essential to elevating scam centres and associated organized crime and corruption as national and regional security concerns. Addressing these threats requires clear recognition at senior levels of government and coordinated messaging across relevant institutions.

- High-level engagement is needed to acknowledge the strategic impact of scam operations and transnational organized crime.
- Raising awareness across government, private sector, and civil society enhances understanding of the risks posed by cyber-enabled fraud, underground banking, and illicit financial flows.

1 UNODC, ASEAN Member States and the People's Republic of China Regional Cooperation Roadmap to Address Transnational Organized Crime and Trafficking in Persons Associated with Casinos and Scam Operations in Southeast Asia, September 2023, available at: https://www.unodc.org/roseap/2023/09/asean-china-action-plan-criminal-scams/story.html.

- National and regional platforms provide opportunities for dialogue, coordination, and collective priority-setting.
- Public education and outreach initiatives help increase understanding of the enabling role of casinos, virtual assets, and other high-risk sectors.
- Criminalizing corrupt acts and enhancing other measures to address and prevent corruption, including by encouraging reporting and protecting reporting persons.

Strengthening regulatory frameworks

Effective prevention and enforcement depend on well-designed legal and regulatory systems that can respond to evolving threats. Closing legislative gaps and aligning frameworks with international standards will help limit the opportunities for criminal exploitation.

- Legal frameworks addressing money laundering, virtual assets, SEZ and casino oversight, and online gambling benefit from periodic review and reform.
- Oversight mechanisms should be applied to financial flows and investment activities in high-risk sectors such as special economic zones and junkets.
- Licensing and supervisory tools are essential for monitoring high-risk financial service providers, particularly those operating through digital platforms.
- Legal provisions that facilitate investigation, prosecution, and asset recovery—while safeguarding victims—strengthen institutional resilience.

Enhancing the technical and operational capacity of enforcement agencies

Enforcement agencies need the tools, skills, and systems required to detect, investigate, and disrupt transnational organized crime. Building institutional capacity and ensuring access to appropriate resources will improve the effectiveness of frontline responses.

- The ability to monitor and investigate threats such as cyber-enabled fraud, underground banking, and misuse of virtual assets should be continuously developed.
- Financial and digital evidence must be collected, preserved, and analyzed in ways that strengthen the integrity of investigations and prosecutions.
- Reducing reliance on victim testimony in trafficking cases through improved investigative techniques is essential to victim-centred justice.
- Specialized training, inter-agency collaboration, and appropriate technology all contribute to stronger enforcement outcomes.

Promoting whole-of-government responses and inter-agency coordination

An integrated national response requires collaboration among all relevant institutions involved in prevention, enforcement, regulation, and protection. Effective coordination mechanisms can bridge institutional silos and improve decision-making.

- National coordination bodies can bring together relevant ministries, enforcement agencies, and oversight institutions.
- Joint training and planning processes improve coherence and shared understanding across sectors.
- Identification, protection, and referral systems for victims of forced criminality should be strengthened and consistently applied.
- Strengthen oversight of border management and accountability for border officials who facilitate trafficking for forced criminality, as well as those who provide protection to scam centres.
- Cooperation among countries of origin, transit, and destination is vital to support safe return, reintegration, and continued assistance for victims.

Advancing practical and operational regional cooperation

Cross-border cooperation is essential to address the transnational nature of scam operations and associated criminal infrastructure. Collective efforts can help prevent displacement, share intelligence, and support enforcement across jurisdictions.

- Mechanisms for timely information exchange and operational coordination should be reinforced at bilateral and regional levels.

- Regional platforms offer a basis for joint investigations and collaboration on high-priority cases.
- Shared research and typology development to improve situational awareness and guide risk-based responses.
- Engagement with multilateral frameworks strengthens mutual legal assistance and supports coordinated approaches beyond the region.



United Nations
Office on Drugs and Crime

Regional Office for Southeast Asia and the Pacific
United Nations Building, 6th floor, Secretariat Building, Raj Damnern Nok Avenue, Bangkok 10200, Thailand
Tel. (66-2) 288-2100 Fax. (66-2) 281-2129 E-mail: unodc-thailandfieldoffice@un.org
Website: http://www.unodc.org/roseap
@UNODC_SEAP