GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME

CRIMINAL CONVERGENCE?

CHINESE-ORIGIN SCAM SYNDICATES AND THEIR REACH INTO SOUTH ASIA

Jason Tower | Radha Barooah

SEPTEMBER 2026

ACKNOWLEDGEMENTS

This briefing note was adapted from an input for the Mapping and Mitigating Telecom Fraud Conference held by the National Forensic Sciences University in Goa, India, in partnership with the UK Government on 7–8 March 2026. It is based on original research conducted by the Global Initiative Against Transnational Organized Crime (GI-TOC) from November 2025 to March 2026 with generous support from the UK Government.

The authors would like to thank the team of researchers whose fieldwork and expertise were integral to this report and the broader project: Poonam Agarwal, Vishal Singh Deo, Saravanan Ravi, Darshatha Gamage and Surendra Shah. Thanks also go to Louise Taylor and Paddy Ginn for their input, and to the GI-TOC's Publications team for their editorial support.

The views expressed and any errors contained herein are strictly those of the authors.

ABOUT THE AUTHORS

Jason Tower is a senior expert at the GI-TOC, where he works on organized crime, security and illicit economies in South East Asia. Since 2019, he has been at the forefront of cutting-edge research on the rise of criminal enclaves hosting industrial scale scam operations across the region.

Radha Barooah is the regional coordinator for the Resilience Fund at the GI-TOC. She works with civil society organizations responding to the localized impacts of organized crime across Asia and the Pacific, and designs and facilitates dialogues on critical organized crime issues in localized contexts. Her work focuses on foregrounding community-rooted perspectives and lived realities of people affected by organized crime.

Cover: © *Ishara S. KODIKARA / AFP via Getty Images*

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

CONTENTS

SUMMARY

Global awareness of the increase in industrial-based cyber scam operations in mainland South East Asia, which use trafficked individuals and forced criminality to target the global population with sophisticated scams, continues to grow. Since 2025, the US, the UK, South Korea, Canada, Australia, Singapore, Thailand, Taiwan and the EU have all scaled up efforts to crack down on this activity, conducting threat assessments, introducing sanctions, indicting key perpetrators and building new law enforcement cooperation on the ground in the region. One of the major limits of the emerging response is the tendency to frame the problem as specific to South East Asia. This response fails to recognize the global reach of the syndicates that are powering the industrial-scale compounds in the current epicentre countries of Myanmar, Laos and Cambodia. Chinese-origin online gambling and scam syndicates have tapped deeply into resources around the globe in order to consolidate their criminal empires in South East Asia.[1] These criminal actors have now also made significant inroads into a wide range of alternative geographies to advance cyber scam operations on a global scale. Of these, South Asia stands out as a region most significantly affected by trafficking in persons for forced criminality into South East Asia, but it is also an emerging operational hub.

This briefing note is one output of a broader study that assesses the extent of the convergence between Chinese-origin cybercrime groups operating in South East Asia and criminal actors across the South Asia region. Focused on India, Nepal and Sri Lanka, it considers the development of cyber scams and online fraud domestically in each country, as well as the local regulatory frameworks and policy responses in each case. This includes a review of available resources – including court and police records and media reports – to analyze the historical involvement of Chinese-origin criminal actors as cyber scams emerged in these countries. All three countries have followed a somewhat similar trajectory in terms of the development of online scams and fraud, but India stands out as having stronger resilience to these forms of crime while also serving as a major provider of external support to other countries in South Asia.

The research identified and documented several patterns of convergence between South Asian, Chinese and South East Asian crime groups that collectively represent major challenges to national, regional and global security. The first of these patterns is the convergence of transnational criminal organizations operating in China and beyond with crime groups in South Asia. This pattern emerged in the late 2010s, coinciding with the migration of Chinese online gambling syndicates across the region. It has intensified particularly since late 2025, as international pressure on cyber scam operations in South East Asia has increased.

Secondly, there is a convergence between cyber scam operations in South East Asia and South Asia-based recruitment and trafficking networks, as well as criminal organizations in South Asia involved in job scams and visitor visa scams. This poses a major human trafficking threat across South Asia, while simultaneously fuelling a rapid increase in the involvement of South Asians and South Asian diaspora groups in cyber scams.

A third convergence occurs at a regional level, where criminal actors from India, Nepal and Sri Lanka are increasingly exploiting the lack of cross-border connectivity between regional law enforcement, regulatory authorities and financial institutions. This enables them to perpetrate scams across borders. Chinese-origin scam syndicates are involved in this regional trend, but with regional crime groups adapting their methodologies and operating structures into their own distinct cyber scam operations.

The study also documented serious regulatory gaps, especially in Sri Lanka. Since 2023, the country has emerged as a new hub for Chinese online gambling operators – serving as a front for online scam operations – who have relocated from the Philippines, Myanmar and Cambodia. Sri Lanka is at serious risk of becoming a hub for industrial-scale cyber scams, and immediate preventative actions are needed to disrupt the criminal consolidation presently underway in the country. This briefing note succinctly summarizes these findings for a policy audience, considers implications for the United Kingdom, and concludes with a series of recommendations.

Key points

- Current responses to the scam industry tend to focus solely on South East Asia, the current epicentre of the problem. This approach fails to recognize that the criminal networks responsible, particularly Chinese-origin syndicates, have a more global reach – with recent inroads seen in South Asia, including in India, Nepal and Sri Lanka.
- Collaboration between criminal groups operating in China and those in South Asia has grown out of the migration of Chinese online gambling syndicates to the region. However, it has intensified since late 2025, with the increased international pressure on South East Asian operations.
- Cyber scam operations in South East Asia and recruitment and trafficking networks in South Asia are collaborating to bring people into South Asia under the false pretences of job opportunities and visitors visas.
- South Asia criminal actors are increasingly exploiting the lack of regional cooperation between law enforcement and regulatory authorities, enabling them to more easily perpetrate scams across borders.
- There are serious regulatory gaps in the response, particularly in Sri Lanka, which has emerged as a hub for Chinese online gambling operators since 2023, and is at risk of becoming a new hub for large-scale cyber scam operations.

RESEARCH FINDINGS

Historical context

Domestic criminal groups have long been active in perpetrating cyber scams in India, Nepal and Sri Lanka. The development of cyber scams has followed a similar trajectory in all three countries, with India standing out as a direct target of cyber scams operations, and criminal groups in Nepal and Sri Lanka often adapting methodologies developed by Indian criminal organizations. The timeline below captures the development of cyber scams in India from 2000 to 2025.

YEAR	EVENT	SIGNIFICANCE	LOCATION
2000–2010	Traditional localized Ponzi and investment fund schemes	Provided a foundation for the emergence of an online fraud ecosystem; initial use of online messaging platforms.	Nationwide
2013–2014	Saradha Group Ponzi scam spreads across West Bengal, Assam and Odisha	Example of one of the first large-scale, multi-state Ponzi scams, resulted in financial losses of US$5 billion.	West Bengal, Assam and Odisha
2016	Kerala ATM skimming fraud (Romanian gang)	First major international cyber fraud involving foreign criminals operating in India	Thiruvananthapuram, Kerala
2016	Shift to online investment scams observed	Digital fraud professionalization begins	Nationwide
2017–2018	Proliferation of romance scams	New methods introduced to target victims on social media	Kerala, Tamil Nadu
2019–2021	Online Ponzi scams emerge (Morris Coin Ponzi)	US$145 million cryptocurrency Ponzi scam	Kerala
2019–2021	Call centre operations emerge	Organized network structures	Hyderabad, Chennai
2022	Retired couple lose US$265 000 to government impersonation scam	Escalation of virtual arrest fraud and impersonation scams	Kerala
2021–2023	Reports of Indians trafficked to South East Asia surge	Indian nationals increasingly integrated into Chinese-origin scam operations in South East Asia	Nationwide
2025	Indian police dismantle India-based trafficking network working with Chinese-origin criminal groups in South East Asia	Evidence of convergence of Indian and Chinese criminal groups	Victims targeted across South Asia

FIGURE 1 Development of scams in India, 2000–2025.

The historical involvement of Chinese-origin cyber scam groups in South Asia dates back to at least 2018. However, their initial attempts to establish themselves at scale in the region were successfully thwarted by law enforcement. An analysis of Indian, Chinese, Sri Lankan and Nepali court records and media reports suggests that Chinese online gambling and cybercrime networks attempted to infiltrate Sri Lanka and Nepal in around 2018. In the case of Nepal, Chinese-origin scam syndicates began moving into the country in significant numbers in 2019, seemingly around the time that Cambodia initiated a crackdown on online gambling operators.[2] In the same year, joint law enforcement operations between Nepal and China appear to have driven many of these criminal groups to northern Myanmar and the Golden Triangle Special Economic Zone (GTSEZ), situated at the border between Laos, Thailand and Myanmar.

A criminal case heard by a court in Guangdong, China, in 2024 documents this development. The case detailed a Chinese-origin syndicate known as the Jian'an Group, which used pig-butchering scams to steal US$2.5 million from 63 victims in China between April and December 2019.[3] According to the case record, the syndicate moved to Myanmar in 2020.[4] A separate case heard by a court in Henan documented a similar operation that relocated from Kathmandu to the GTSEZ at around the same time.[5] Reports from Nepali sources also evidence significant crackdowns on scam operations in 2019, including the arrest of 122 Chinese nationals in reportedly 'the biggest crackdown on foreign nationals in [the country's] history'.[6]

Human trafficking and growing embeddedness of Chinese-origin crime groups in South Asia

The demand from Chinese-origin scam syndicates operating in Cambodia, Laos and Myanmar for young, English-speakers made South Asia a natural location for recruitment operations. Our research has documented the development of a trafficking pipeline from the region since in 2021. The GI-TOC estimates that more than 30 000 South Asians are currently being held in scam compounds in mainland South East Asia. In the case of India alone, data compiled for this study from India's Ministry of Home Affairs shows that 30 000 out of 73 000 Indian nationals failed to return home after visiting South East Asian countries between 2022 and 2024. This gap raises concerns that some of these missing individuals are being held in scam centres across the region.

Among the schemes targeting South Asians are visitor visa and job scams. They are often tricked into paying for their own travel to the UAE, Oman or another destination in the Middle East, where they enter on a visitor visa, only to later be trafficked to South East Asia for forced criminality in cyber scam centres. Since 2024, Chinese-origin criminal groups have also used government impersonation scams to lure Sri Lankans into South East Asia-based scam centres.[7] Chinese crime groups have also established regional linkages that facilitate the trafficking of South Asian victims using India as a transit point. For example, counter-trafficking NGOs in Nepal reported that Nepali victims had transited through New Delhi on the way to compounds in South East Asia.[8]

Chinese-origin scam syndicates have built strong ties with regional crime networks in South Asia for the purposes of trafficking. In all three focus countries, the GI-TOC found evidence of Chinese-origin scam syndicates directly employing local trafficking and smuggling syndicates to draw South Asians into South East Asia. In India, for example, Nilesh Purohit (aka 'The Ghost'), who police claim is the senior leader of a trafficking network, was arrested in Gujarat in November 2025. The government of Gujarat has alleged that Purohit sent more than 500 people from India, Sri Lanka and several other countries into cyber slavery in Myanmar and Cambodia.[9] Similar patterns were observed in the other two countries, with the GI-TOC finding that the Chinese crime groups were paying US$3 250 and US$5 000 per victim.

Unregulated online gambling

Crackdowns in South East Asian countries since 2023 have generated renewed interest in South Asia on the part of Chinese-origin online gambling and scam syndicates. When the Philippines began to crack down on offshore online gambling in 2022, tens of thousands of Chinese nationals departed the country.[10] This corresponded with the rapid liberalization of the casino industry in Sri Lanka, beginning also in 2022.[11] On-the-ground interviews conducted by the GI-TOC date the arrival of Chinese-origin online gambling syndicates to the same year. Meanwhile, casino industry sources support these claims, with a recent Asia Gaming Brief report uncovering evidence of large numbers of relocations from Philippine offshore gaming operations.[12] In 2024, Sri Lankan authorities began to report that Chinese nationals were emerging as the top players in the country.[13]

A sudden surge in tourist arrivals between 2023 and 2025, especially from countries associated with industrial-scale cyber-scam operations, offers further evidence of the migration of online gambling and cyber-scam syndicates to Sri Lanka. According to official Sri Lankan immigration data, tourist arrivals in the country grew by over 100% between 2022 and 2023, and this upward trend has continued, with a further 50% increase from 2023 to 2025. During the same period, arrivals from Myanmar and Cambodia surged by 120% and 105%, respectively.[14]

Reports of online-gambling and cyber-scam syndicates relocating to Sri Lanka from the Philippines and other countries emerged around the period leading up to the opening of the City of Dreams casino in Sri Lanka. Although this does not establish a causal relationship, it is an indication that Sri Lanka's expanding gambling sector has increased the country's attractiveness to these operations. Significantly, the City of Dreams has been central to the gambling industry in the Philippines since the opening of its Manila property in 2015, hosting a wide range of VIP gambling services and Chinese speaking junket operators.[15] Bodu.co, a Chinese-language gambling-industry media and information platform, reported that the opening of the casino represented a hallmark in the emergence of Sri Lanka as a 'BC heaven' (in Chinese, the abbreviation 'BC' is used to refer to online gambling and scams – from bocai, meaning 'gambling').[16]

Sri Lanka is now at considerable risk of being transformed into a hub for Chinese-origin scam syndicates, with criminal actors exploiting online casino operations and business process outsourcing facilities to establish cyber-scam operations. In 2024 and 2025, the police raided two major online scam operations in the Colombo area, leading to the arrest of 340 foreigners, most of whom were Chinese nationals.[17] Despite these actions, and additional raids in 2026, the same buildings are still being used by so-called 'tech companies' harbouring large numbers of Chinese, Vietnamese and Indonesian nationals. Many of these individuals appear to have ties to or are hosted by business process outsourcing (BPO) companies registered inside the Port City Colombo, a special economic zone.[18] This raises concerns that criminal actors might be exploiting preferential policies offered by the Port City to scale their operations in the country. Meanwhile recruitment advertisements for a broad range of online gambling and associated technology firms continue to be found across a wide range of Telegram channels (see below).

Chinese-origin criminal actors are also tapping into a growing network of over-the-counter crypto exchanges operating in Sri Lanka, which provide online gambling and scam operations with the tools needed to move funds within the country and globally. Public Telegram channels established for the Chinese-speaking community in Sri Lanka have grown rapidly, with one such platform now maintaining 90 000 members. This platform advertises a range of scam-adjacent services, as well as Chinese-language offshore online gambling sites, which are seemingly being operated from Sri Lanka. Of significant concern is the fact that an online gambling platform previously advertising within Myanmar's KK Park scam compound, known as U8.com, has opened offices in Sri Lanka. U8 can also be seen advertising on taxis and billboards along the main highway between downtown Colombo and the airport (see the images).[19]

Top: U8.com is seen advertising on taxis and billboards along the main highway between downtown Colombo and the airport. Bottom: Advertisements for U8 on buildings in Myanmar's KK Park, November 2024. *Photos supplied*

A collective recruitment advertisement for nine different brands of Chinese online gambling operations promoted by EqualOcean Technology Group for Sri Lanka. *Photo: Telegram*

Regulatory capacity and gaps

Within South Asia, India stands out as having the kinds of world-class institutions and capacities needed to monitor and disrupt cybercrime. Nevertheless, numbers of registered complaints continue to rise dramatically. India has contributed significantly in the battle to halt the spread of cyber scams into Nepal, often as part of efforts to combat Chinese-origin criminal influence in the country. Indian law enforcement efforts in collaboration with Nepal police have highlighted how criminals have created an extensive transnational network involving mule accounts – bank or payment accounts used to receive and move money on behalf of criminals – in India that link to scam syndicates from China and Cambodia operating in Nepal. These scam syndicates in turn have financial operations extending into Dubai.[20] Meanwhile, less attention has been paid to the situation in Sri Lanka.

Metric	July 2024	July 2025	October 2025	Growth
CFCFRMS amount saved	US$265 million	US$603 million	US$819 million	209%
Complaints handled	760 000	1.7 million	2.3 million	203%

FIGURE 2 The Indian Cybercrime Coordination Centre's financial impact and complaint metrics show exponential growth in fraud prevention from July 2024 to October 2025.

India faces several challenges in its efforts to address cyber scams. First among these is the tension between jurisdictional constraints and the need for rapid enforcement action. Cybercriminals frequently operate across multiple domestic and international jurisdictions, exploiting differences in legal systems, investigative procedures and enforcement gaps. Traditional mechanisms for cooperation, such as letters rogatory, can take months to process, and evidence can decay quickly. This is one reason why real-time or near-real-time liaison (through working arrangements and dedicated liaisons) is now being emphasized in new memoranda of understanding (MoUs). Secondly, criminals increasingly route proceeds through cryptocurrencies and across multiple jurisdictions, complicating traditional bank-centric tracing. INTERPOL campaigns are adapting, but capacity building remains necessary. Thirdly, for sustained cooperation, consistent standards for digital forensics, evidence handling and cross-border warrants are still being developed; the Cybercrime Coordination Centre and newer bilateral MoUs explicitly list capacity building as a priority.

Capacity to combat cybercrime in Sri Lanka is similarly limited, and the legal framework is outdated. The Computer Crime Act of 2007 remains Sri Lanka's primary criminal statute addressing cybercrime,[21] but it was enacted before cryptocurrency, cloud computing and social media fraud emerged as major threats. It contains no express provisions addressing digital asset fraud, AI-generated deception or platform-facilitated scam recruitment, the three mechanisms most commonly used by contemporary cyber scam networks. The Gambling Regulatory Authority Act of 2025 is one of the most significant recent reforms to Sri Lanka's digital regulatory landscape, consolidating piecemeal gambling regulation under a single independent regulator, the Gambling Regulatory Authority, and explicitly bringing 'digital gambling' and online interactive gaming within its scope.[22] A major challenge, however, is the rollout and implementation of the legislation, as well as the need to catch up with the large number of operators already active in the country.[23]

Nepal faces similar challenges to Sri Lanka with legacy legislation. The Electronic Transactions Act (2008) remains the foundational statute for prosecuting digital offences in Nepal.[24] Originally drafted to facilitate e-commerce and ensure the security of electronic transactions, it has been repurposed without revision as the de facto 'Cybercrime Act'.[25]

Gap area	Legal status	Weaknesses/impact
Digital evidence rules	Weak/outdated	There are no modern digital evidence standards, which impacts forensic validity with chain of custody lacking detail, leading to loss of evidence.
Crypto assets	None	The absence of specialized crypto offence regimes results in difficulty seizing stolen virtual assets.
Mule network	Indirect coverage	There is no explicit prohibition for intermediaries facilitating fraud, and large numbers of facilitators are not held accountable.
Business process outsourcing compliance	Non-existent	The lack of compliance standards or background checks results in legitimate businesses being used as fronts for scam operations.
Encrypted platforms oversight	Weak	There is no lawful interception framework governing Telegram and the dark web. The government relies on blanket bans rather than targeted investigations.
Criminal liability	Lenient	Serious cybercrimes are not sufficiently punished.

FIGURE 3 Challenges in Nepal's legal framework to combat cyber scams.

Implications for the United Kingdom

India has historically been utilized as a hub for cyber scam operations targeting the UK.[26] Nevertheless, law enforcement cooperation between India and the UK is increasingly sophisticated. Representatives of India's Criminal Bureau of Investigation and of local law enforcement based in areas where scam hubs targeting UK nationals have previously been identified have indicated that there are now far fewer complaints related to UK nationals than in previous years. In 2025, there were significant joint operations in the Noida Special Economic Zone, in Uttar Pradesh, targeting call centres scamming UK nationals.[27] This illustrates the ongoing threat, but also the responsiveness of existing cooperative frameworks.

GI-TOC researchers were unable to identify evidence of Chinese-origin criminal groups using India to target UK nationals with the types of scams being perpetrated from South East Asia-based compounds. Nevertheless, the risk of this happening is increasingly clear. A trafficking victim interviewed in Uttar Pradesh, who was recently rescued and repatriated from a scam centre in Myanmar, stated that the scam syndicate he was lured into had forced him and other South Asians under their control to directly target UK nationals. He said he was forced to use the profile of a female entrepreneur from Singapore to maintain daily contact with 30–35 UK nationals on WhatsApp. This underscores the growing risk that South Asians may increasingly be exploited by South East Asia-based scam syndicates to target British nationals, and that South Asians involved in the scam syndicates may adapt the methodologies deployed by Chinese-origin criminal groups to target the UK.[28]

In the case of Sri Lanka, GI-TOC researchers were unable to find evidence of the country being used as a hub to directly target the UK. That said, the growing presence of offshore online gambling syndicates and their adjacent underground banking facilities points to growing threats to the global financial system, including the UK. A secondary threat was identified through interviews with repatriated Sri Lankans, including one who spent several months inside a compound in the GTSEZ. According to this account, the scam syndicate specialized in 'niche market' scams, in this case targeting the LGBTQ+ community using common social media platforms serving that community, such as Romeo and Grindr. The individual was forced to establish profiles as a young, attractive man on the platform and target a global population of men, particularly trying to identify individuals whose gender identity was not publicly known. This demographic was targeted explicitly because of a perceived higher probability of success and a lower probability that victims would bring cases to law enforcement due to fear of stigmatization. The syndicate targeted wealthy individuals regardless of the country in which they were based. Such scams are a shared threat to the UK, India, Sri Lanka and Nepal.

CONCLUSION AND RECOMMENDATIONS

The ongoing development of what is often referred to as the South East Asia cyber-scam economy demonstrates the adaptability of the transnational criminal networks behind it. Although industrial-scale scam compounds remain concentrated in South East Asia, the transnational criminal networks that operate them are not geographically confined to this region. This research shows that Chinese-origin scam syndicates are increasingly connected to criminal actors, recruitment networks, financial infrastructure and online gambling operations across South Asia. India, Nepal and Sri Lanka are affected in different ways, but together they illustrate how the scam economy is becoming increasingly transnational, decentralized and resilient to enforcement pressure.

As is illustrated by the discussion of India, South Asia is already an important source of people trafficked into scam compounds, including through increasingly sophisticated regional recruitment and trafficking networks. At the same time, criminal actors in South Asia are adapting scam methodologies developed elsewhere, while transnational networks exploit gaps between national law enforcement agencies, financial systems and regulatory regimes. Perhaps most urgently, developments in Sri Lanka demonstrate how enforcement pressure in one jurisdiction can displace criminal networks to another. The emergence of Chinese-origin scam syndicates alongside or embedded in online gambling operations and BPO facilities creates conditions in which a new regional hub could consolidate if preventive action is delayed.

As such, cyber scams cannot be addressed as a South East Asian problem alone. Responses focused narrowly on dismantling compounds risk shifting criminal activity rather than disrupting the networks that enable it. Governments and international partners must increasingly target the scam economy as a connected transnational system, and build mechanisms for rapid intelligence sharing, financial disruption and coordinated enforcement across regions.

India

India's capacity to address cyber scams as well as human trafficking has expanded exponentially over the past five years, but significant gaps remain, especially as cybercriminals have introduced more sophisticated scams, money laundering operations and recruitment tactics. Key recommendations identified through the study for India are as follows:

- Build frameworks (both working arrangements and MoUs) so that operational requests travel fast and with legal clarity, particularly for cases that involve multiple jurisdictions across India or have a transnational element. This can help India in overcoming major challenges in prosecution cross-state and/or transnational cyber scam cases, where India presently faces a low conviction rate.[29]
- Establish multilateral frameworks for operations that can apply pressure across the full range of geographic nodes involved in transnational cyber scams. Share insights from these operations at scale, including through public channels.
- Allocate more resources to tackling threats related to online scams in Sri Lanka. Consider also investments in strengthening Sri Lanka's regulation of the casino industry as a means of addressing potential threats to Indian nationals that might stem from unregulated offshore online gambling sites.
- Consider establishing regional platforms for intelligence sharing, joint law enforcement operations and broader cooperation targeted at addressing the growing regional nexus of online scams and fraud. This is especially important given that the GI-TOC has detected similar threats emerging in Pakistan, Bangladesh and beyond.

Nepal

Nepal faces growing exposure to both cyber scams and the trafficking of its citizens into scam compounds abroad. Its response is constrained by an outdated legal framework, limited technical capacity and low levels of public awareness. Key recommendations include:

- Update and modernize the Electronic Transactions Act (2008) to address the threats of modern cyber scams, including offences related to crypto currencies and digital assets, cross-border financial fraud, fintech fraud, phishing and malware-specific crimes.
- Build the technical capacity of law enforcement at all levels to identify, investigate and prosecute cybercrimes across Nepal instead of concentrating capacity in the capital.
- The complete ban of cryptocurrency in Nepal has neither deterred nor prevented its use, especially in laundering proceeds from cyber scams and other illicit economies. Regulatory bodies must consider models that enable the tracing of digital assets essential in anti-money-laundering efforts.
- Relevant government agencies, including the Ministry of Foreign Affairs, the Department of Immigration and the Anti-trafficking Bureau, must track the location of Nepali citizens who have travelled to South East Asian countries and Gulf countries on visitor visas and have not returned. This would establish a baseline of Nepali citizens potentially trafficked abroad, whether into scam centres or other forms of labour trafficking. Given the presence of scam centres in South East Asia and the high number of foreign nationals forced to work in them, the data could help reveal whether they have been recruited as well. Enforce labour permits and insurance verification at the airport to prevent citizens from falling into trafficking traps.
- Cooperate with the Indian government on monitoring Nepali citizens travelling to South East Asian countries from Indian territory by establishing a specific mechanism at Indian immigration points that assesses labour permits and insurance verifications for Nepali citizens.
- Introduce rigorous public awareness campaigns with the intention to improve digital literacy of Nepali citizens as well as financial literacy to deter the establishment of mule accounts.
- Introduce specific anti-mule-account provisions in relevant banking, electronic transactions and anti-money laundering legislation. These provisions should establish liability for persons who knowingly or recklessly provide, sell, rent, transfer or permit the use of their bank or digital-payment accounts to facilitate cyber fraud or the laundering of criminal proceeds, while protecting account holders whose accounts or identities were used without their knowledge or consent.

Sri Lanka

Sri Lanka faces a rapidly growing threat from cyber scams, particularly as Chinese-origin online gambling and scam syndicates establish a greater presence in the country. Significant gaps in cybercrime legislation, regulation and enforcement capacity, particularly related to online gambling and BPOs increase the risk that Sri Lanka could develop into a major hub for cyber scams.

To address the connections between human trafficking and recruitment into the cyber scam industry:

- The Sri Lanka Bureau of Foreign Employment, in coordination with the Sri Lanka Telecommunications Regulatory Commission and the Criminal Investigation Department, should establish a dedicated digital intelligence monitoring unit to identify and flag fraudulent overseas employment advertisements on high-risk platforms. Takedown requests and platform-level cooperation agreements with Facebook/Meta and Telegram should be pursued, and stronger regulation introduced.
- Sri Lanka should develop and publicly maintain an accessible registry of identified fraudulent recruitment entities, potentially in coordination with the International Organization for Migration (IOM) and/or INTERPOL.
- The Anti-Human-Trafficking Task Force should formalize structured information-sharing protocols with Thailand, the IOM and Cambodian counterparts on active trafficking pipelines targeting Sri Lankan nationals. The Sri Lankan embassy in Bangkok – which has been the de facto operational hub for repatriations – should receive dedicated anti-trafficking resources commensurate with this operational role.
- Sri Lanka's anti-trafficking legislation should be amended to create express provisions for targeting cyber-enabled trafficking modalities.

To address the growing online casino–scam nexus:

- Tighten regulations around foreign work permits, particularly in the online gambling sector. Consider limitations on the number of foreign workers that companies can host in the country.
- Establish and empower a dedicated oversight committee for the gambling sector.
- Deepen law enforcement cooperation with countries that have experienced struggles with the regulation of offshore online gambling, especially the Philippines. This should include establishing direct intelligence-sharing channels that might assist with due diligence proceedings around casino licensing and immigration background checks.
- Based on the experience of the Philippines, conduct detailed cost–benefit analysis of the offshore online gambling industry. In conjunction with this, develop a detailed mitigation strategy to prevent offshore online gambling operations and BPOs from being used as fronts for online scam operations.
- Consider a ban on offshore online gambling operations.
- Strengthen regulation of crypto-currency platforms and enforce laws related to foreign currency exchange platforms.

To combat online scams more broadly:

- Enact a comprehensive cyber fraud act that consolidates digital scam offences, cryptocurrency misuse, AI-enabled deception and platform liability provisions within a single modern statute.
- Invest in dedicated cyber fraud investigation units within police, with specialized digital forensics and cryptocurrency tracing capabilities.

The international response

- In order to effectively combat the cyber scam operations that are presently operating at industrial scale in mainland South East Asia, establishing a global response, including intelligence-sharing platforms, will be critical. This could potentially build on the SHIELD platform established in Thailand in July 2026.[30]
- Consider prioritizing preventative actions in Sri Lanka, including supporting the development of a comprehensive regulatory framework to govern physical and online casinos as well as BPOs in the country. To maximize effectiveness, this might be conducted with technical support from India.
- Establish a monitoring facility that tracks the involvement of Chinese-origin cybercrime groups across the globe. As a first step, baseline studies should be conducted in present hotspot countries in South Asia.
- Provide technical assistance to Sri Lanka and Nepal for the regulation and monitoring of cryptocurrency and for digital forensics. This might also potentially be done in conjunction with India's Cybercrime Coordination Centre.

NOTES

1 Chinese-origin syndicates are defined as those with Chinese leadership that have, over the past five years, integrated a large number of South East and South Asian nationals, as well as individuals from many other countries into their ranks.

2 Bradley J Murg, How Cambodia's online gambling ban sparked the Great Chinese Exodus of 2019 – and why Beijing is fine with it, South China Morning Post, 5 September 2019, https://www.scmp.com/comment/opinion/article/3025687/how-cambodias-online-gambling-ban-sparked-great-chinese-exodus-2019.

3 Court decision, People's Court of Panyu City, Guangdong Province, 2024, Record: 2024 – 0113 – 1013 (in Chinese), 19 January 2026, https://wenshu.court.gov.cn.

4 Ibid.

5 Court decision, People's Court of Xixia County, Henan Province, Criminal Judgment in the Fraud Case of Zhao [surname redacted], 2024-1323-86 (in Chinese), 29 March 2024, https://wenshu.court.gov.cn.

6 WION, Nepal police detains 122 Chinese nationals for engaging in suspicious activities, YouTube, 25 December 2019, https://youtu.be/tK2ayYir4k0?si=U4yEdP46Qt-6spOe.

7 Interview with a trafficking victim, Colombo, Sri Lanka, 2 May 2026.

8 See also: US Department of State, 2023 Trafficking in Persons Report: Nepal, https://www.state.gov/reports/2023-trafficking-in-persons-report/nepal.

9 Official release, Gujarat CID-Crime's Cyber Centre of Excellence (CCoE), reproduced in: 'Mastermind' of 'cyber slavery' racket arrested: Gujarat Police, The Indian Express, 19 November 2025, https://indianexpress.com/article/cities/ahmedabad/mastermind-of-cyber-slavery-racket-arrested-police-10373294.

10 Philippines to shut 175 offshore gambling firms, deport 40,000 Chinese workers, Reuters, 26 September 2022, https://www.scmp.com/news/asia/southeast-asia/article/3193909/philippines-deport-40000-chinese-workers-crackdown-online.

11 Government of Sri Lanka, Gazette Extraordinary No. 2295/10: Casino Business Licensing Regulation No. 1 of 2022, 31 August 2022, https://www.ird.gov.lk/en/publications/Gazette_Documents/2022_2295-10_E.pdf.

12 Viviana Chan, Former POGO-linked operators reportedly shift to Sri Lanka's Port City, Asia Gaming Brief, 9 August 2026, https://agbrief.com/news/sri-lanka/09/08/2026/former-pogo-linked-operators-reportedly-shift-to-sri-lankas-port-city.

13 Sulochana Ramia Mohan, Money extortion: Chinese nationals top list in SL – police, Ceylon Today, 12 October 2024, https://ceylontoday.lk/2024/10/12/money-extortion-chinese-nationals-top-list-in-sl-police.

14 See Sri Lanka Tourism Development Authority, Tourism arrival reports, https://www.sltda.gov.lk/en/monthly-tourist-arrivals-reports.

15 Marianne Carandang, Melco Crown unveils City of Dreams Manila, TTG Asia, 10 October 2013, https://www.ttgasia.com/2013/10/10/melco-crown-unveils-city-of-dreams-manila.

16 International casino opens: Sri Lanka as yet another BC paradise, Bodu News, 28 June 2025, https://www.bodu365.co/a/187721.html.

17 130 Chinese telecom fraud suspects arrested in Sri Lanka! The first group of 85 are returned to Guangzhou, Sohu News, 21 June 2025, https://www.sohu.com/a/906412092_206880.

18 Through field research, GI-TOC researchers identified that large numbers of foreign nationals were working out of two buildings in Colombo, which the police had raided for cyber scams in 2025, and had employee badges that read 'Port City BPO, Ltd'. Port City BPO, Ltd was designated by the Sri Lankan cabinet in 2024 as a BPO that provides shared services for the overseas entertainment industry. See: Sri Lanka Cabinet Decision, 8 April 2024, https://www.cabinetoffice.gov.lk/cab/index.

php?Itemid=49&dID=12495&id=16&lang=en&option=com_content&view=article.

19 U8's own Telegram platform makes mention of its operations, while branding and advertising are visible across Sri Lanka.

20 Nepal based investment scam exposed as Mangaluru police arrest 11, The 420, 5 February 2026, https://the420.in/mangaluru-police-nepal-investment-fraud-cybercrime-investigation-india.

21 Parliament of Sri Lanka, Computer Crimes Act, No. 24 of 2007, https://www.parliament.lk/en/acts-of-parliament.

22 Parliament of Sri Lanka, Gambling Regulatory Authority Act, No. 17 of 2025, https://www.parliament.lk/uploads/acts/gbills/english/6393.pdf.

23 Majorie Preston, Sri Lanka gambling regulator to launch by mid-2026, iGaming Business, 20 October 2025, https://igamingbusiness.com/casino/sri-lanka-gaming-regulator-launch-june-2026.

24 Government of Nepal, The Electronic Transaction Act 2008, https://tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf.

25 Ibid.

26 Prasun Sonwalker, UK grappling with cyber scamsters based in India, Hindustan Times, 18 March 2019, https://www.hindustantimes.com/india-news/uk-grappling-with-cyber-scamsters-based-in-india/story-B00KgxrlmGK0XynXP5mHvI.html.

27 Central Bureau of Investigation (India), CBI busts cyber fraud syndicate targeting UK and Australian citizens, 8 July 2025, https://cbi.gov.in/press-detail/NzExMQ%3D%3D.

28 Interview with a trafficking victim in Uttar Pradesh, 20 January 2026.

29 India recently successfully prosecuted a criminal involved in a digital arrest case, the first time this has happened. See: Nine get life imprisonment in Bengal for 'digital arrest' fraud, The Hindu, 19 July 2025, https://www.thehindu.com/news/national/west-bengal/9-sentenced-to-life-in-prison-in-bengal-for-digital-arrest-scam/article69827846.ece.

30 See: Thai police launch SHIELD platform to track scam networks, Migrant Times, 10 July 2026, https://migrantimes.com/crisis-displacement/09-07-2026/thai-police-launch-shield-platform-to-track-scam-networks.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 800 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net