Cracking Southeast Asia's Scam Economy

Washington and London's recent unprecedented actions showed what global coordination can achieve – and what remains to be done.

Last month, the United States and United Kingdom mounted one of the largest coordinated law enforcement operations ever conducted targeting Southeast Asia-based actors, taking aim at the finances of a major network in the region's cyber-scamming industry. The U.S. Treasury sanctioned 146 individuals and entities linked to Cambodia's Prince Group, chaired by businessman Chen Zhi, and unsealed indictments alleging that companies tied to the conglomerate were involved in online fraud, human trafficking, and money laundering. Investigators seized 127,000 bitcoins worth around $14 billion, while the United Kingdom froze high-value real estate in London.

Over the past decade, online fraud operations across Southeast Asia have generated vast profits while defrauding victims around the world. Americans alone lost an estimated $10 billion to these scams in 2024.

The U.S.-U.K. measures suggest the fusion of political power, private wealth, and illicit enterprise in Cambodia – a pattern repeated across the region. In the weeks since, governments implicated in the scam economy have moved to signal action. Yet those efforts are constrained by a deeper problem: these illicit industries are woven into the fabric of political and economic power itself, making genuine enforcement perilous for regimes that depend on them.

Southeast Asia and the Globalized Illicit Economy

The rise of Southeast Asia's scam economy can be traced to the convergence of at least three forces. The first is the entrenched systems of rent extraction and protection that have long shaped governance across the region. The second is the surge of Chinese grey capital after 2010, as money flowed offshore through real estate, casinos, and online gambling ventures that blurred the line between speculation and crime. The third is the rapid expansion of digital and crypto-based finance, which allowed illicit profits to circulate globally through opaque and weakly regulated payment systems. Each of these forces evolved independently, but together they transformed online fraud from small, decentralized criminal ventures into a transnational industry embedded within political and economic power.

Across much of Southeast Asia, power rests on personal authority and control over resources rather than on formal institutions. Politicians and officials rely on business allies, military officials, and local brokers to raise money, deliver loyalty, and manage disputes. These relationships have deep roots in the way states were built, from colonial administration and Cold War alliances to later efforts to hold together diverse territories with limited bureaucratic capacity. Over time, they produced political systems that adapt easily, drawing new sources of income, including illicit ones, into established networks of profit and protection.

The surge of Chinese capital after 2010 entered these systems rather than creating new ones. Inside China, successive anti-corruption and capital-control measures, including under Xi Jinping, pushed grey and speculative money abroad. After Beijing's 2012 anti-corruption campaign, investors sought safer jurisdictions for unregistered wealth, while the 2018–2019

crackdown on online gambling and stricter limits on cross-border transfers accelerated the outflow. Cambodia, Laos, Myanmar, and the Philippines became preferred destinations: investors could secure land, licenses, and security guarantees through government officials, tycoons, and military intermediaries. Casinos, industrial zones, and real estate developments became the main conduits, as developers partnered with local elites who could provide protection and official cover.

The COVID-19 pandemic deepened this transformation. When borders closed and tourism collapsed, casino developments and real estate projects were repurposed into scam compounds. Workforces that had once served the gambling sector were replaced with trafficked and coerced labor recruited from across the region.

The spread of cryptocurrency and digital payments gave the system unprecedented reach. Proceeds from scams are passed through mule bank accounts, exchanged to virtual currency, moved through various crypto wallets and mixed with other funds, laundered by over-the-counter brokers, and reintroduced into formal banking channels. The same platforms that power legitimate commerce now move illicit funds across borders in seconds. These technologies did not replace older forms of corruption; they extended them, linking Southeast Asia's entrenched rent economies to transnational circuits of illicit accumulation and to the global financial systems that sustain them.

By 2023, this machinery had transformed parts of the region into the command center of a global industry. The United Nations and regional law enforcement estimated that scam compounds employed hundreds of thousands of people and generated billions of dollars annually. Victims were spread globally. Profits moved through offshore jurisdictions. But the physical infrastructure – the compounds, guards, and managers – remained embedded in the region's political economies, where local authority and international capital converge.

The State-Crime Nexus

Cambodia sits at the heart of Southeast Asia's scam economy. Over several decades, the ruling Cambodian People's Party has fused state power with private business, allowing tycoons to profit from monopoly contracts and political protection. What began as war and post-conflict economy built on timber and land concessions shifted toward Chinese-backed real estate and casino investment. Online gambling was banned in 2019, prompting many operators to leave. However, the gambling ban coincided with a rapid rise in online scam operations, and the infrastructure created by the gambling boom was easily repurposed for scamming. These operations have depended heavily on trafficked workers to target victims around the world.

These operations could not have thrived without high-level protection. Scam compounds were built on properties owned by politically connected businessmen, foreign operators were granted citizenship and honors, and investigations were quietly dropped, if they commenced at all. The allegations levied by the U.S. and the U.K. against Chen Zhi of the Prince Group would seem to exemplify this nexus of power, money, and impunity. Chen's recent indictment and the seizure of billions in cryptocurrency appear to reveal the scale of the scam profits that investigators have linked to his network, reflecting the wider entanglement of illicit finance with Cambodia's economy.

Several blockchain analytics firms have also reported large-scale laundering of scam proceeds via a payments platform reportedly linked to relatives of the prime minister. The platform was

subsequently blocked from the U.S. financial system in October, yet no public measures have been taken against its owners. By 2025, U.S. officials were referring to Cambodia as a "state sponsor" of human trafficking.

The U.S.-U.K. actions against Chen Zhi and the Prince Group have left the Cambodian government scrambling to contain the fallout. A run on Prince Bank, as savers rushed to withdraw their money, forced the government to issue assurances to prevent contagion across the economy. Around the same time, Thai authorities froze the assets of tycoon Ly Yong Phat – one of Cambodia's most powerful business figures and a key regime financier – further increasing the pressure on Phnom Penh's patronage networks.

In response, senior officials have tried to project resolve, using high-level meetings and bilateral forums to talk tough on scams despite the industry's deep entanglement with the national economy. Open-source investigations now suggest a duck-and-cover operation is underway, with scam workers relocating from sanctioned compounds to new sites along the Vietnamese border. Yet it remains unclear how the Cambodian government can meaningfully rein in an industry that so deeply permeates its economy while generating vast revenues for regime elites.

Myanmar's scam centers emerged from decades of civil war and divided authority. Along the country's borders, ethnic armed groups and pro-military militias have long run their own administrations, collecting taxes, licensing businesses, and policing territory. Cyber-scamming became another revenue stream in these zones, joining narcotics, logging, and jade.

The town of Shwe Kokko in Kayin (Karen) State shows how this system works. Though the political dynamics change often and rapidly there, the Karen Border Guard Force, a militia under the governance structure of the army but effectively operating autonomously, partnered with Chinese investors to build a walled enclave of casinos and scam operations, complete with private guards and power lines. Revenues funded weapons and recruitment, strengthening the militia's hand in its dealings with the military. In Shan State, an ethnic armed group attacked military-backed scam centers in 2023 as it reclaimed previously lost territory. Across Myanmar's borderlands, scam money has become part of the war economy, reshaping who holds power.

Recent activity at the infamous complex KK Park, located near Myawaddy on the Thai border, has drawn international attention in the wake of the sanctions. According to recent state media reports, the junta's forces shut down operations at KK Park late last month, but details are murky. Yet analysts emphasize that the crackdown appears highly managed. While the military proclaimed a "clearance" of KK Park, credible accounts indicate that bosses were informed in advance and left, then gates were opened. More than 1,500 people fled to Thailand, but others were moved to different compounds. The pattern illustrates the resilience of scam-hub economies in border zones where control is fragmented, and elite networks are intertwined with illicit business.

Elsewhere in the region, Laos's scam economy thrives under a one-party system that has long traded access and protection for investment. Lacking domestic industries and burdened by debt, the government has relied on concessionary and other deals that hand vast tracts of land and resources to foreign investors. This permissive environment has encouraged illicit economies to grow alongside formal ones, often under official protection.

The clearest example is the Golden Triangle Special Economic Zone (GTSEZ), run by Chinese businessman Zhao Wei. Despite U.S. sanctions for trafficking and money laundering, Zhao was awarded a state medal in 2024 for his "contributions" to local policing. The zone functions as a private enclave – with its own casinos, security, and economy – where scams and trafficking operate openly under the protection of Lao authorities. Rather than confronting the problem, the state has absorbed it, relying on these rents to sustain political loyalty and foreign exchange inflows.

Here, too, enforcement has been partial. In August 2024, Lao authorities issued an ultimatum to scam operators to dismantle hundreds of online fraud factories in the GTSEZ by 25 August, in cooperation with Chinese authorities worried about the abuse of Chinese nationals. The zone has long been flagged for human trafficking, online fraud, and money laundering via its casino and real estate operations. The raids and deportations affected low-level staff rather than the core networks, and ownership of the zone remains unchanged. Consequently, the "crackdown" functions more as stage management — demonstrating willingness to act while leaving the principal actors and structures intact. Following a period of raids and inspections in 2023 to 2024, scam operations continued, and in the last month there have once again been reports of raids in the zone.

The most successful enforcement to date has occurred in the Philippines. Here cyber-scamming grew out of the country's offshore gambling boom. Under President Rodrigo Duterte, the government created a licensing system for "Philippine Offshore Gaming Operators," or POGOs, which drew heavy Chinese investment and generated tax revenues for both national and local governments. Weak oversight and the country's system of decentralized patronage gave local politicians broad discretion over permits and enforcement. Many used it to extract rents from operators or shield them from investigation.

By 2023, national raids revealed how deeply these networks had penetrated the state. In the province of Tarlac, investigators linked Mayor Alice Guo to a large scam compound in her municipality. She is now facing charges related to her role in the operation. Attention has fallen on her origins, as it emerged that she was actually born in China but obtained citizenship documents using a false identity. However, the bigger story here is how she and her network were able to dominate both business and politics in the locality, operating a massive scam operation in plain sight. Similar raids in Pampanga, Las Piñas, and Pasay uncovered trafficked workers and evidence of official complicity.

Unlike in Cambodia, Laos, or Myanmar, enforcement in the Philippines has been real and sustained. The Marcos administration's 2024 ban on POGOs (signed into law in 2025) was preceded and followed by repeated police and immigration raids, prosecutions of local officials, and the deportation of thousands of workers. Some large operations have been permanently shut down, and public scrutiny has made political protection costlier. Yet many operators have rebranded or moved underground, sometimes using the same buildings and personnel, or finding new bases to conceal their operations. Real enforcement, in this case, has constrained but not eliminated an industry that thrives in the gaps of the country's fragmented political order.

When Crime Becomes Governance

The result is that, across Southeast Asia, cyber-scamming has become part of how power and money work. In Cambodia, it sustains elite patronage; in Myanmar, it bankrolls military,

militias, and warlords; in Laos, it operates with official protection; and in the Philippines, it thrived in the spaces between national and local authority. These operations rarely flourish without state involvement. Officials license, protect, or profit from the very networks they are supposed to police. In many cases, the profits and political utility make sustained enforcement unlikely.

What began in the region is now moving outward. The same playbook that built scam compounds in Sihanoukville and Shwe Kokko is appearing beyond Southeast Asia – in parts of the Caucasus, West Africa, and Latin America – adapting to local systems of protection and rent-seeking. Profits move through cryptocurrency wallets, offshore companies, and property markets in Singapore and London. U.N. and regional law-enforcement estimates suggest that hundreds of thousands of people are still trapped in compounds generating billions in annual proceeds. The system endures because it links local brokers to a global infrastructure of finance and technology, fusing digital innovation with entrenched corruption.

The joint U.S.-U.K. action against Cambodia's Prince Group showed what coordinated pressure can achieve. By targeting the financial architecture of scamming – the companies, bank relationships, and London property connecting illicit profits to the formal economy – authorities reached the actors who profit most. But such efforts remain rare. Cybercrime thrives because it serves political interests at home and because the global financial system enables it abroad. Western banks, property markets, and cryptocurrency exchanges continue to absorb illicit proceeds with few questions asked. Until those channels are closed, enforcement in Southeast Asia will only shift the problem elsewhere.

Effective action will require more than moral condemnation. It will demand sustained enforcement of the type seen in the U.S.-U.K. sanctions and action to regulate how global finance, including cryptocurrency, interacts with corrupt governance. The crackdown on Cambodia's Prince Group therefore was an important first step. Turning it into a precedent will require sustained coordination – not only with Southeast Asian governments, but with the financial centers that make their economies, and their scams, possible.

Author Bio

Neil Loughlin is Associate Professor of Comparative Politics at City, St George's, University of London. His research focuses on authoritarian politics and the political economy of development. He is the author of *The Politics of Coercion: State and Regime Making in Cambodia* (Cornell University Press, 2024) and is currently working on a book about crime and politics in Southeast Asia.