INSTITUTE FOR STRATEGIC POLICY

The Need for Concerted Global Efforts Against Transnational Crime in Cambodia

Occasional Paper
No. 1/2026

Institute for Strategic Policy (ISP)
January 2026

Abstract

Cambodia has emerged as a primary global epicenter for transnational organized crime, characterized by a sophisticated convergence of cyber-enabled fraud, human trafficking, and industrial-scale money laundering. This paper examines the operational mechanics of "scam compounds," the actors involved, and the socio-economic impact of an illicit industry now estimated to generate billions of dollars—rivaling the nation's formal GDP.

Without serious and concerted international intervention, the "scam state" model risks becoming a permanent and counter-productive fixture of the regional economy, while the circles of sufferings of innocent victims and abuses of human rights will continue to expand.

Introduction

The landscape of transnational crime in Southeast Asia underwent a radical shift following the 2019 ban on online gambling and the subsequent COVID-19 pandemic. In Cambodia, these factors catalyzed the repurposing of casino infrastructure into fortified "scam compounds." As of 2025, these sites represent a "criminal service economy" where human rights abuses are not merely incidental but a core component of the business model.[1]

The Mechanics of Exploitation

At the heart of this crisis are large-scale online fraud operations, specifically "pig butchering" (romance-investment) scams and illegal gambling. These activities rely on a workforce of approximately 100,000 to 150,000 individuals, many of whom are victims of human trafficking lured by fraudulent job advertisements for high-paying tech roles.[2]

Once inside the compounds—often located in Sihanoukville, Phnom Penh, Poipet and elsewhere along the Thai-Cambodian border—workers face systemic human rights abuses. Reports from Amnesty International and the U.S. Department of State detail a "living nightmare" of:

- **Forced Labor and Abductions:** Victims are held against their will, with passports confiscated.
- **Physical Torture:** Punishment for failing to meet scam quotas includes beatings, electrocution, and solitary confinement.[3]
- **Severe Abuse:** Credible reports have emerged regarding sexual violence and, in extreme cases, the illegal sale of human organs to satisfy "debts" or as a byproduct of the trafficking cycle.[4]

Perpetrators and Political Complicity

The actors behind these syndicates are predominantly transnational criminal organizations (TCOs) with roots in China, often operating through local conglomerates. In October 2025, the U.S. Treasury Department designated the **Prince Group**, led by Chen Zhi, as a TCO, accusing it of orchestrating a global empire built on forced labor.[5] Another key entity, **Huione Group**, has been identified as a critical "connective tissue" for the industry, facilitating the laundering of billions in illicit proceeds through cryptocurrency and underground banking.[6]

The persistence of these operations points to significant state complicity. Many compounds are located within Special Economic Zones (SEZs) owned by politically connected tycoons. For instance, the **MDS Thmorda SEZ** in Pursat Province and owned by a tycoon by the name of Try Pheap, has been identified by the US State Department and UNODC as a site for large-scale scam operations.[7] Other SEZs that strong evidence suggests the existence of scam centers inside include **Sihanoukville Special Economic Zone (SSEZ)**, **Bavet SEZs** (Svay Rieng), **Manhattan SEZ**, **Tai Seng Bavet SEZ**, near the Vietnamese border, and **Koh Kong SEZ**. The U.S. State Department's 2024 *Trafficking in Persons Report* noted that "officials reportedly inappropriately penalized victims for crimes committed as a direct result of being trafficked," while high-ranking advisors were found to have direct financial interests in properties used by scammers.[8]

Economic Value and Money Laundering

The scale of this shadow economy is staggering. The United Nations Office on Drugs and Crime (UNODC) estimates that cyber-scam operations in Cambodia generate between **USD 12.5 billion and USD 19 billion annually**, which is equivalent to roughly 30% to 60% of the country's formal GDP.[9]

These funds are managed through a sophisticated "interconnected ecosystem" of:

1. **Cryptocurrency:** In 2025, the U.S. DOJ conducted a record seizure of approximately **USD 15 billion** in Bitcoin linked to Cambodian scam networks.[10]
2. **Underground Banking:** Traditional banking systems are bypassed using "mule" accounts and various forms of money laundering.
3. **Real Estate:** Profits are laundered into high-value assets in neighboring countries and globally, including property development projects in Bangkok, London mansions and Singaporean luxury properties.[11]

Conclusion

Cambodia's scam industry has evolved from a local nuisance into a global security threat. The integration of generative AI and deepfakes has further empowered these syndicates to target victims worldwide with unprecedented efficiency. Without aggressive international intervention, the "scam state" model risks becoming a permanent and counter-productive fixture of the regional economy, fueled by the sufferings of trafficked workers and innocent scam victims.

Recommendations for the International Community

To address the "scam state" crisis in Cambodia with the required proactive and offensive stance, the international community must transition from mere observation to active disruption. These recommendations are grounded in the principles of the **United Nations Convention against Transnational Organized Crime (UNTOC)** and the newly adopted **Hanoi Convention (2025)**, which emphasize that sovereignty does not provide a shield for state-sponsored or state-abetted criminality.[12]

Recommendations

1. Implementation of "Extraterritorial Judicial Task Forces"

The international community, led by victims' home nations (such as China, Vietnam, and the US), should establish joint task forces authorized to exercise **Extraterritorial**

Jurisdiction. Under the principle of *aut dedere aut judicare* (extradite or prosecute), states must aggressively pursue the masterminds of criminal entities, such as those running the Prince and Huione Groups, in any jurisdiction they enter.

- **Offensive Action:** Issue "Red Notices" through INTERPOL specifically targeting the beneficial owners of SEZs where scam compounds operate, effectively making them "international pariahs" unable to use global travel or financial infrastructure.

2. Financial Asphyxiation through "Secondary Sanctions"

Moving beyond individual designations, major economies such as the US and EU should apply **Secondary Sanctions** against any regional bank—including those in neighboring Thailand or Vietnam—that facilitates transactions for Cambodian "scam-linked" conglomerates.

- **Proactive Measure:** The **Financial Action Task Force (FATF)** should not only re-list Cambodia on the "Grey List" but issue a "Call for Action" (Blacklist), mandating global financial institutions to apply enhanced due diligence that makes Cambodian international wire transfers prohibitively expensive and complicated in procedures, thereby "pricing out" the criminal economy.[13]

3. "Digital Blockade" of Scam Infrastructure

The international community must pressure global Internet Service Providers (ISPs) and satellite companies to implement a coordinated **Digital Blockade** on IP ranges associated with known scam compounds.

- **Offensive Action:** Utilizing the **Hanoi Convention's** framework for real-time data sharing, tech giants (e.g., Apple, Google, Meta) should be legally required to geofence and disable all "work-related" apps and crypto-wallets operating within the coordinates of documented slave compounds.[14]

4. "Asset Recovery Offensive" (Operation Stolen Wealth)

The UNODC's **StAR (Stolen Asset Recovery) Initiative** should launch a dedicated "Cambodia Cell" to proactively freeze and seize luxury real estate and "mule" accounts worldwide.

- **Realistic Enforcement:** Shift the burden of proof to the accused through **Unexplained Wealth Orders (UWOs)**. For instance, if a politically exposed person (PEP) in Cambodia cannot prove the legal origin of a **USD 50 million**

London mansion, the asset should be liquidated to fund a **Victim Reparation Fund**.[15]

5. Conditionality of Regional Trade Agreements

In order to be effective in addressing the problem of transnational crimes in Cambodia, ASEAN must, at least temporarily, waive its "non-interference" policy. Formal legal frameworks such as the **ASEAN Treaty on Mutual Legal Assistance in Criminal Matters (2004)** should be activated to launch criminal investigations, including money laundering, in trade and financial transactions between Cambodia and other ASEAN Member States. Other trade preferences arrangements such as the ones under the **RCEP (Regional Comprehensive Economic Partnership)** should also be made contingent on Cambodia to allow independent international inspectors access to SEZs.

- **Offensive Diplomacy:** If access is denied, member states should authorize measures, such as imposing embargos on trade and financial transactions with Cambodia or "targeted border closures" at the borders of Thailand and Vietnam to halt the flow of technical hardware, technical personnel and "human cargo" that feeds the compounds.

Footnotes

1. UNODC, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud*, October 2024.
2. Amnesty International, *"I Was Someone Else's Property": Slavery, human trafficking and torture in Cambodia's Scamming Compounds*, June 2025.
3. U.S. Department of State, *2024 Country Reports on Human Rights Practices: Cambodia*.
4. *Security Management Magazine*, "Outrage Over Cambodian Scam Centers Grows," October 16, 2025.
5. U.S. Department of the Treasury, *U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia*, October 14, 2025.
6. Business and Human Rights Centre, *Report reveals alleged complicity in transnational crimes*, May 16, 2025.
7. UNODC, Inflection Point: Global Implications of Scam Centres, 2025.
8. U.S. Department of State, *2024 Trafficking in Persons Report: Cambodia*.
9. UNODC, *Inflection Point: Global Implications of Scam Centres*, April 2025.
10. TRM Labs, *Historic U.S.–U.K. Operation Targets Southeast Asia's Scam Compounds*, October 2025.
11. *The Diplomat*, "Singapore Police Seize $115M in Assets Tied to Cambodia's Prince Group," November 3, 2025.
12. United Nations, Convention against Transnational Organized Crime (UNTOC), 2000; Hanoi Convention on Cybercrime, October 2025.

13. FATF, Targeted Financial Sanctions Related to Proliferation Financing, Updated 2025.
14. Hanoi Convention, Article 22: "Cooperation in Real-time Collection of Traffic Data," 2025.
15. UNODC/World Bank, Stolen Asset Recovery (StAR) Initiative: Annual Report, 2025.

Bibliography

Amnesty International. (2025). *"I Was Someone Else's Property": Slavery, human trafficking and torture in Cambodia's Scamming Compounds*.

The Diplomat. (2025). *Singapore Police Seize $115M in Assets Tied to Cambodia's Prince Group*.

FATF. (2025). Updated Standards on Beneficial Ownership and Transparency.

Hanoi Convention. (2025). United Nations Convention against Cybercrime.

United Nations Office on Drugs and Crime (UNODC). (2024). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia*.

United Nations Office on Drugs and Crime (UNODC). (2025). *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*.

UNODC. (2025). Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia.

U.S. Department of State. (2024). *Trafficking in Persons Report: Cambodia*.

U.S. Department of the Treasury. (2025). *Treasury Designates Prince Group Transnational Criminal Organization.*

Contact:
Mr. Pana Janviroj
Executive Director
Institute for Strategic Policy
Bangkok, Thailand.
Jpana88@gmail.com