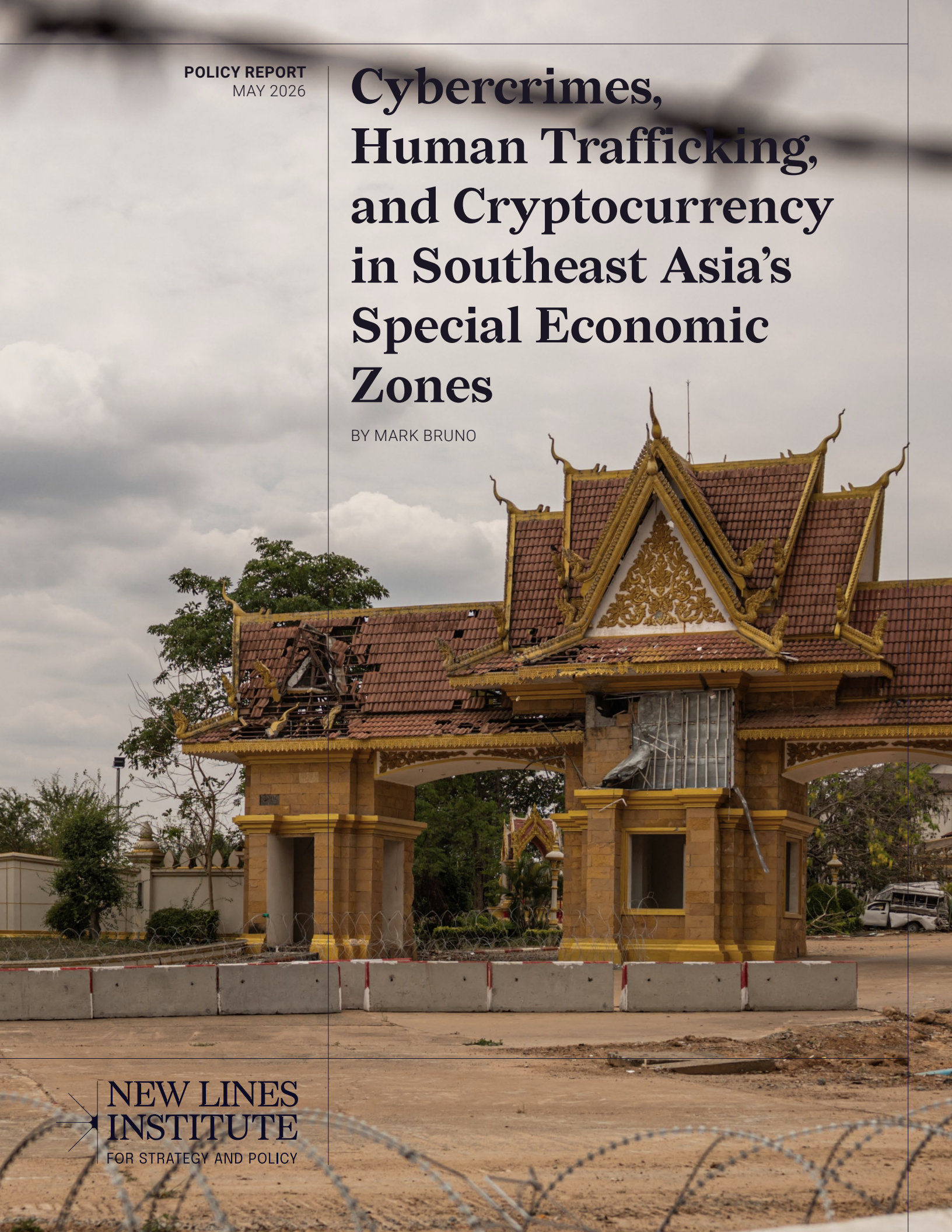
POLICY REPORT
MAY 2026

Cybercrimes, Human Trafficking, and Cryptocurrency in Southeast Asia's Special Economic Zones

BY MARK BRUNO



NEW LINES INSTITUTE
FOR STRATEGY AND POLICY

THE NEW LINES INSTITUTE FOR STRATEGY AND POLICY

Our mission is to provoke principled and transformative leadership based on peace and security, global communities, character, stewardship, and development.

Our purpose is to shape U.S. foreign policy based on a deep understanding of regional geopolitics and the value systems of those regions. remove it over time.

The content and views expressed in this report are those of the author and should not be taken to reflect an official policy or position of New Lines Institute for Strategy and Policy.

Cover Image: The entrance to O'Smach scam compound on the Thai-Cambodia border on March 12, 2026 in Oddar Meanchey, Cambodia. (Getty Images)

CONTENTS

EXECUTIVE SUMMARY

Southeast Asia's special economic ones (SEZs) were designed to attract investment through deregulation and streamlined governance. Those same features have made them ideal substrate for growing transnational criminal networks. Across Myanmar, Cambodia, Laos, and the Philippines, Chinese-led syndicates have embedded industrial-scale cyber-fraud operations inside these SEZs, generating an estimated $50 billion - 75 billion annually while relying on a traffic workforce of at least 300,000. In 2024 alone, U.S. victims lost more than $10 billion to such schemes.

This report maps operations, and the political economies sustaining them, in Laos' Golden Triangle SEZ, Myanmar's Shwe Kokko and KK Park, Cambodia's Sihanoukville and Thmor Da, the Philippines' Clark Freeport, and East Timor's emerging Oecusse Digital Trade Zone. It traces the money-laundering infrastructure, armed group protection arrangements, and legal exceptionalism that have made meaningful enforcement persistently elusive. It also examines how forced criminality structurally blurs the line between victim and perpetrator and how existing countermeasures have prioritized visible disruption over the systemic dismantling of this ecosystem.

Recent U.S. actions, including from the Office of Foreign Asset Control, have targeted entities such as the Prince Group and Huione Network, in attempts to cut this ecosystem from the U.S. financial sector. The November 2025 launch of the Scam Center Strike Force is a step in the right direction for these efforts, but the momentum needs to be codified and institutionalized.

This report argues that durable progress will require reframing these ecosystems as hybrid security threats, targeting both the operators themselves and their financial and political enablers. Victim protection should also be treated as a driver of these efforts, as well as a valued intelligence asset, and not just a humanitarian afterthought.

Introduction

In early 2024, the Indian Ministry of External Affairs announced the rescue of 250 of its citizens[1] from cyber slavery in Cambodian scam compounds. While the operation was a rare human rights victory, it represented only a fraction of the estimated 100,000 people trapped in similar facilities[2] across Cambodia, including roughly 5,000 Indian nationals[3] still believed to be in bondage.

Their accounts described a now-familiar pattern: workers lured by fraudulent online job advertisements, transported across borders, and coerced into carrying out cyber fraud on an industrial scale. Those brought from India were reportedly forced to conduct "pig-butchering" investment scams, a long-term form of investment fraud where scammers build a relationship with victims before convincing them to invest in a fraudulent platform or product.

The victims' experiences mirror those of hundreds of thousands across the Mekong region confined in heavily fortified compounds, where passports are confiscated, movement is controlled, and refusal to comply is met with violence and threats of re-trafficking. Survivors in Myanmar allege that underperforming workers even face forced organ harvesting.[4] At least 300,000 people[5] across Cambodia, Myanmar, Laos, and the Philippines are now trafficked or coerced into this work, forming the backbone of a shadow economy estimated to generate $50 billion to $75 billion[6] annually, rivaling the illegal narcotics sector in profitability.

1 Ministry of External Affairs, Government of India. "Official Spokesperson's Response to Media Queries Regarding Indians Stuck in Cambodia." March 30, 2024. https://www.mea.gov.in/response-to-queries.htm?dtl/37760/Official_Spokespersons_response_to_media_queries_regarding_Indians_stuck_in_Cambodia.

2 United Nations News. "Hundreds of Thousands Trafficked into Online Criminality across SE Asia." August 29, 2023. https://news.un.org/en/story/2023/08/1140187.

3 Indian Express. "5,000 Indians in Cambodia, Forced into Cyber Scams; MHA Takes Note." March 29, 2024. https://indianexpress.com/article/india/5000-indians-in-cambodia-forced-into-cyber-scams-mha-takes-note-9239156/.

4 Organized Crime and Corruption Reporting Project. "Myanmar Says It Repatriated 70,000 Foreigners Forced to Work in Scam Centers." OCCRP, December 2025. https://www.occrp.org/en/news/myanmar-says-it-repatriated-70000-foreigners-forced-to-work-in-scam-centers.

5 Southeast Asia Public Policy Institute. Towards an ASEAN Response to Scams. September 2025. https://seapublicpolicy.org/wp-content/uploads/2025/09/SEAPPI_Towards-an-ASEAN-response-to-scams_September-2025.pdf.

6 U.S.-China Economic and Security Review Commission. China's Exploitation of Scam Centers in Southeast Asia. Staff Research Report. Washington, DC: USCC, July 2025. https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf.

These compounds have expanded dramatically[7] in recent years, clustering in the region's deregulated special economic zones (SEZs), where lax oversight provides ideal conditions for transnational criminal networks. Revenues from cyber-fraud operations now sustain armed groups in Myanmar's civil war, have intersected with fighting[8] along the Thai-Cambodian border, and contributed to frictions[9] between China and the Philippines.

While it faces far less trafficking risk, the United States suffers disproportionate financial losses. More than $10 billion[10] was stolen from U.S. victims in 2024 alone, according to U.S. Treasury Department estimates. Given its past contribution to multilateral efforts,[11] financial exposure, unmatched intelligence, and sanctions capabilities, the United States is uniquely positioned to coordinate a sustained regional response. China, the dominant regional power, has intervened with mixed results,[12] mounting highly visible operations in Myanmar but failing to stem the broader crisis. Without American leadership, these hybrid criminal-industrial complexes will continue eroding governance, destabilizing regional security, and undermining global financial systems.

This report will examine five different SEZ ecosystems. Laos' Golden Triangle SEZ, Myanmar's Shwe Kokko and KK Park, Cambodia's Sihanoukville and Thmor Da, and Clark Freeport in the Philippines all provide examples of an SEZ that has been co-opted or captured by transnational criminal networks. East Timor's Oecusse Digital Trade Zone, demonstrates a developing replication case, showing that the model is spreading to new jurisdictions before legal or enforcement measures can be implemented. Across these sites, the report maps the money laundering infrastructures sustaining these operations, and the legal and jurisdictional obstacles that have made meaningful enforcement elusive. It then turns to the normative failures that have left trafficked workers without protection and the policy levers available to the United States and its regional partners to disrupt both the illicit economy and the networks that supply it with human labor.

Deregulation into Criminal Ecosystems

Transnational criminal organizations, largely Chinese-led networks,[13] have transformed parts of Southeast Asia's SEZs into global epicenters of cyber-enabled fraud and human trafficking. Conceived as engines of economic modernization, SEZs were designed to attract foreign investment[14] through deregulation, tax exemptions, and streamlined governance. Yet these same features – minimal oversight, privatized administration, and preferential legal treatment for investors – have created ideal conditions for criminal groups to build industrial-scale fraud operations shielded from state intervention.

This pattern is visible across the Mekong subregion. Laos's Golden Triangle SEZ, effectively controlled by sanctioned Chinese businessman[15] Zhao Wei,

7 Global Initiative Against Transnational Organized Crime. "Compound Crime: Cyber Scam Operations in Southeast Asia." May 2025. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

8 Foreign Policy. "Thailand-Cambodia War and Pig Butchering Scams." September 12, 2025. https://foreignpolicy.com/2025/09/12/thailand-cambodia-war-pig-butchering-scams/.

9 Wang, Fan. "Alice Guo: Philippines Jails 'Chinese Spy Mayor' for Life," November 20, 2025. https://www.bbc.com/news/articles/cx2l20jzp30o.

10 U.S. Department of the Treasury. "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams." Press release, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237.

11 Global Initiative Against Transnational Organized Crime. "Joint US-India Focus on Cyber Scams Is a Chance to Curb a Global Fraud Epidemic." 2025. https://globalinitiative.net/analysis/joint-us-india-focus-on-cyber-scams-is-a-chance-to-curb-a-global-fraud-epidemic/.

12 Hutt, David. "What Is the West's Response to China's Role in Myanmar War?" Dw.Com, November 29, 2024. https://www.dw.com/en/what-is-the-wests-response-to-chinas-role-in-myanmar-war/a-70922423.

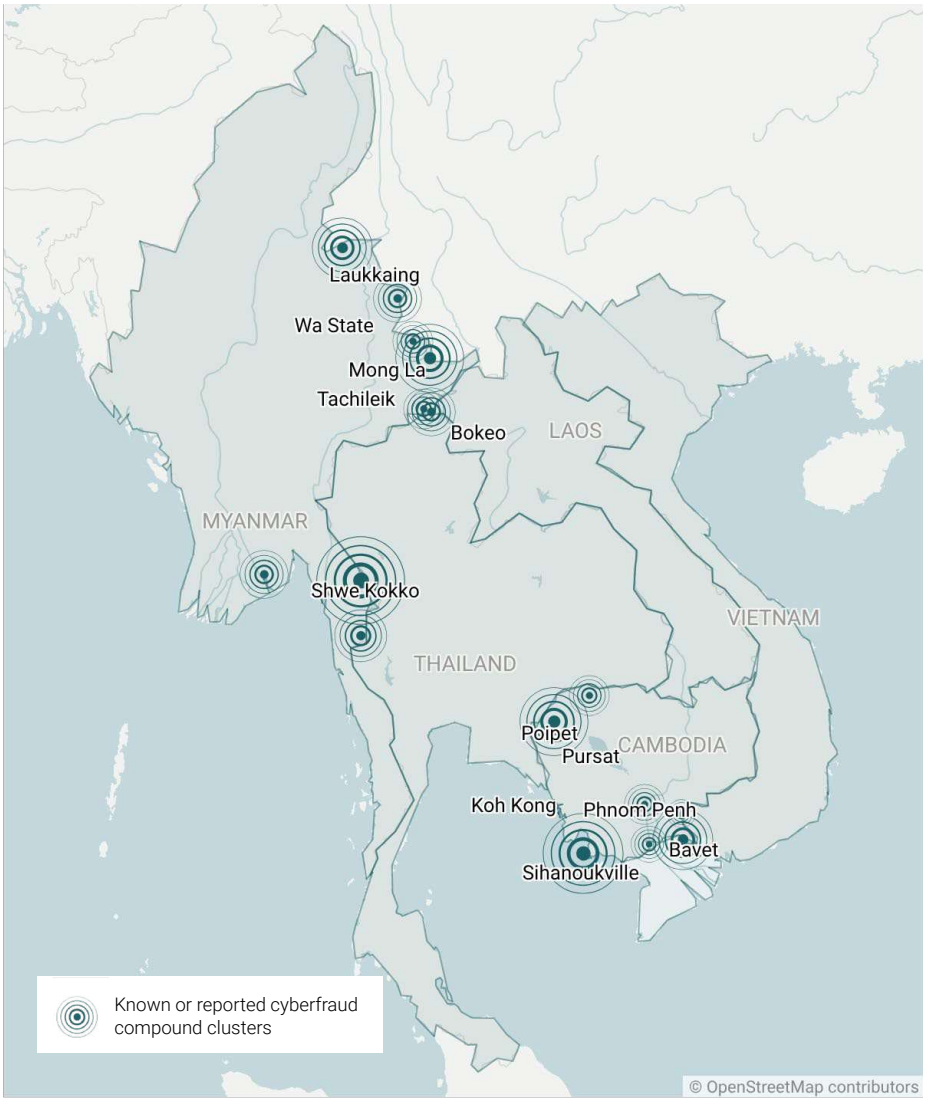
13 U.S.-China Economic and Security Review Commission. China's Exploitation of Scam Centers in Southeast Asia. Staff Research Report. Washington, DC: USCC, July 2025. https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf.

14 Asian Development Bank. Special Economic Zones for Shared Prosperity in BIMP-EAGA. Manila: ADB, 2024. https://www.adb.org/sites/default/files/publication/840041/special-economic-zones-shared-prosperity-bimp-eaga.pdf.

15 Strangio, Sebastian. "Laos Bestows National Development Award on Sanctioned Chinese 'Crime Boss.'" The Diplomat, December 10, 2024. https://thediplomat.com/2024/12/laos-bestows-national-development-award-on-sanctioned-chinese-crime-boss/.

functions as a semi-autonomous enclave[16] with its own security forces, currency circulation, and border controls. Cambodia's Thmor Da SEZ, linked to illegal logging tycoon[17] Try Pheap, and Myanmar's Shwe Kokko and KK Park developments under pro-junta Karen Border Guard Force[18] operate similarly.

Cyberoperations in the Mekong Region



Created with Datawrapper

Source: UNODC

The COVID-19 pandemic accelerated this transformation. As casinos and tourist complexes across Cambodia, Laos, and Myanmar shuttered in 2021, their infrastructure was repurposed into cybercrime compounds.[19] Dormitories once used for casino staff or construction workers became holding centers for trafficked laborers. Recruitment networks expanded across South and Southeast Asia, luring victims through false job postings for IT work, marketing roles, or overseas call-center employment. Upon arrival, workers were confined within high-walled facilities,[20] stripped of their passports, and forced to defraud

16 United Nations Office on Drugs and Crime. Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, 2025. https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

17 Civil Forum For Asset Recovery. Sanctions Watch. "Try Pheap." 2025. https://sanctionswatch.cifar.eu/try-pheap.

18 U.S. Department of the Treasury. "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams." Press release, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237.

19 Global Initiative Against Transnational Organized Crime. Compound Crime: Cyber Scam Operations in Southeast Asia. Geneva: GI-TOC, May 2025. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

20 Mc, Ali. "Abused, Exploited: How Two Africans Became Trapped in a Cyber-scam in Laos." Al Jazeera, May 31, 2025. https://www.aljazeera.com/features/2025/5/30/each-person-had-10-phones-trapped-in-a-cyber-scam-centre-in-laos.

victims worldwide through romance scams, crypto-investment schemes, and high-pressure extortion pipelines.

The Philippines represents a parallel but connected case. Although not structured around SEZs in the same way as the Mekong states, its online gambling industry, the Philippine Offshore Gaming Operators (POGOs), has created its own quasi-enclave environment enabled by weak regulation, rapid cash flows, and significant Chinese criminal infiltration.[21]

POGO hubs in metro Manila and Luzon have imitated the Mekong model of abusing these trafficked foreign workers and then laundering their proceeds through local banks and real-estate markets. Their continued operation relies on corruption networks to avoid enforcement. While some POGO operations have been shut down, many simply fragment, relocate, or rebrand the same adaptive behavior in SEZ-based criminal operations elsewhere in the region.

This ecosystem holds substantial consequences for regional security. In Myanmar, revenues from cyber-fraud compounds help finance armed groups[22] across the civil war's frontlines, including junta-aligned militias such as the Karen National Army, which has faced targeted U.S. Treasury sanctions for its involvement.[23]

In Laos and Cambodia, criminal networks are more actively tied to government interests, as income from these compounds makes up over 30% and 40% of the countries' GDPs,[24] respectively. In the Philippines, POGO-linked transnational criminal organizations have entrenched themselves within local enforcement and regulatory bodies, and positioning themselves between Manila and Beijing.

Despite periodic crackdowns, the scam economy continues to adapt and relocate. Underground banking channels, cryptocurrency-based laundering, and the ability to shift operations across permissive jurisdictions allow these networks to siphon tens of billions of dollars annually with little disruption. Border officials, police units, and licensing authorities frequently rent out enforcement or protection to private actors, further eroding state control and enabling transnational criminal organizations to entrench themselves across multiple sectors of the regional economy.

The Infrastructure

The permissiveness of Southeast Asia's SEZs extends to cyberspace. These organizations utilize sophisticated legal, financial, and digital infrastructure, operating as vertically integrated criminal economies built to extract, launder, and reinvest capital with minimal friction. This is all done despite several layers of sanctions and nominal rejection by their local governments.

At the front end, the scamming victims are targeted across Asia, North America, and Europe, often through romance or investment schemes. The content is increasingly tailored using AI-enabled chat tools, synthetic profile photos, and even deepfake video impersonation[25] for high-stakes social engineering. In more advanced iterations of pig-butchering scams, operators

21 Global Initiative Against Transnational Organized Crime. Compound Crime: Cyber Scam Operations in Southeast Asia. Geneva: GI-TOC, May 2025. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

22 United Nations Office on Drugs and Crime. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

23 U.S. Department of the Treasury. "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams." Press release, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237.

24 Global Initiative Against Transnational Organized Crime. Compound Crime: Cyber Scam Operations in Southeast Asia. Geneva: GI-TOC, May 2025. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

25 United Nations Office on Drugs and Crime. "Billion-dollar cyberfraud industry expands in Southeast Asia as criminals adopt new technologies." UNODC Regional Office for Southeast Asia and the Pacific, October 2024. https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html.

now run customer relationship management software to track victim behavior and manage longer-term fraud pipelines.

Once money is extracted, typically through bank transfers, crypto payments, or a combination, it's moved through laundering networks designed to minimize exposure. Proceeds are often converted immediately into stablecoins like U.S. Dollar Tether and routed through dozens of wallets. Over-the-counter brokers across Cambodia, Laos, and the Philippines act as informal clearinghouses, and allow scammers to swap crypto for local currencies or Chinese renminbi while evading know-your-customer systems, which are used to identify and establish chain-of-custody to users conducting these transactions. Offshore mixer services such as Tornado Cash[26] are used to further obfuscate these asset trails. Mixer services function by pooling cryptocurrency from an entire network of users and randomly redistributing them. Some of these brokers are tied to informal Chinese banking networks, giving criminals the ability to move capital seamlessly across borders.

CASE STUDY: THE PRINCE GROUP/HUIONE NETWORK

Prince Holding Group is a Cambodia-based conglomerate that U.S. and U.K. authorities have publicly described as a transnational criminal organization[27] for its ties to forced-labor scam compounds and large-scale pig butchering crypto investment fraud. Reporting centers on compounds linked to Jin Bei Group, a luxury hotel and casino operation connected to Prince Group, with additional sites throughout Cambodian SEZs.

Huione Group and its marketplace arm, formerly known as Huione Guarantee and later branded Haowang Guarantee, is a critical money-laundering node[28] that combines a payments firm (Huione Pay), a virtual-asset service provider (Huione Crypto), and an online "guarantee" marketplace offering illicit services and tools. According to FinCEN,[29] the broader Huione network laundered at least $4 billion in illicit proceeds between August 2021 and January 2025.

Chen Zhi is a Chinese-born, Cambodia-based businessman and chairman of the Prince Group who U.S. authorities say is the leader of a transnational criminal organization and large-scale cryptocurrency investment fraud.[30] Chen has denied wrongdoing, but he has been sanctioned by the United States and named in civil forfeiture and criminal filings connected to billions of dollars in alleged fraud.

1 PLACEMENT

Victim conversion into crypto

2 ENABLER LAYER

Service procurement via the "guarantee" market-place

Money Laundering Flow of Prince Holding Group

Victims are steered into "crypto investment" scams and directed to send funds (often crypto) into scam-controlled wallets/exchanges. U.S. and U.K. authorities claim Prince Group-linked compounds are key operational hubs for these schemes.[31]

Scam operators use Huione/Haowang Telegram marketplaces to buy money movement and laundering services, plus "fraud infrastructure" such as scam website development, victim data storage, and deception tooling. Investigators at blockchain analytics firm Elliptic document vendors explicitly advertising

26 Reynolds, Sam. "Crypto.com's Stolen Ether Being Mixed Through Tornado Cash." Coindesk, May 11, 2023. https://www.coindesk.com/business/2022/01/18/cryptocoms-stolen-ether-being-laundered-via-tornado-cash.

27 U.S. Department of the Treasury. "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia." Press release, October 14, 2025. https://home.treasury.gov/news/press-releases/sb0278.

28 Financial Crimes Enforcement Network. "FinCEN Finds Cambodia-Based Huione Group to Be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists." Press release, May 1, 2025. https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern.

29 Financial Crimes Enforcement Network. "FinCEN Finds Cambodia-Based Huione Group to Be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists." Press release, May 1, 2025. https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern.

30 Lamb, Kate. "Who Are Chen Zhi and the Prince Group, Accused by the US and UK of Large-scale Scam Operations?" The Guardian, October 17, 2025. https://www.theguardian.com/world/2025/oct/17/chen-zhi-prince-group-cambodia-cyber-crime-sanctioned.

31 U.S. Department of the Treasury. "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia." Press release, October 14, 2025. https://home.treasury.gov/news/press-releases/sb0278.

laundering,[32] moving victim funds cross-border and converting between cash, stablecoins (notably USDT), and Chinese payment apps. The same investigation[33] by Elliptic describes a concrete example where a Huione-linked payments actor agreed to handle $2 million of fraud-derived funds for a 10.5% fee, demonstrative of the group's fee-for-service laundering at scale.

3 DENIABILITY LAYER

Stablecoin-heavy circulation and rapid cross-border movement

These markets run heavily on stablecoins: Elliptic estimates Huione Guarantee/Haowang-related wallets have received at least $24 billion in crypto[34]; Telegram later removed Huione/Haowang and Xinbi[35] channels after reporting that the two markets facilitated more than $35 billion in stablecoin transactions.

4 INTEGRATION

Cash-out

Funds are cashed out through payment services or over-the-counter brokers and then integrated into ostensibly legitimate businesses and assets. The U.S. Department of Treasury's Prince Group action,[36] which sanctioned 146 targets within the group's network, defined this as a "legitimization" layer through corporate structures and investments, while also flagging a Laos-based bitcoin mining operation, Warp Data Technology Lao Sole Co., that allegedly funneled large quantities of bitcoin into wallets controlled by Chen Zhi, providing a pseudo-legitimate on-chain cover story.

Connectivity in isolated or militarized zones has been sustained through cellular spoofing, where fake cell towers intercept and mimic legitimate network connections and, in some cases, satellite internet. Myanmar's military and affiliated militias were found using Starlink terminals[37] to maintain compound operations, even in blackout conditions. These arrangements allowed the compounds to continue operations despite degraded regional infrastructure.

Gambling infrastructure continues to serve as the central conduit for layering illicit proceeds. Criminal operators have rerouted illicit capital through these newer nodes, particularly in Shwe Kokko, Sihanoukville, and the Golden Triangle SEZ. Casinos and junket accounts allow for funds to be deposited, briefly cycled through nominal betting, and withdrawn as "clean" gambling winnings. In parallel, an informal network of cross-border luxury and real estate[38] trades function as downstream channels to repatriate and legitimize value inside China.[39]

The scam economy's durability depends on its local integration. In Cambodia, Try Pheap and the Thmor Da SEZ have hosted a number of these operations, while Chinese criminal networks operating under She Zhijiang established their own real-estate developments, complete with office parks and dormitories. In She Zhijiang's case, these were all funded as Belt-and-Road Initiative

---

32 Elliptic. "Huione Guarantee: The multi-billion dollar marketplace used by online scammers." Elliptic Blog. July 9, 2024. https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin.

33 Elliptic. "Huione Guarantee: The multi-billion dollar marketplace used by online scammers." Elliptic Blog. July 9, 2024. https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin.

34 Elliptic. "Huione: the company behind the largest ever illicit online marketplace has launched a stablecoin." Elliptic Blog. January 14, 2024 https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin

35 Crawley, Jamie. "Telegram Shuts Down $27B Illicit Marketplace, Haowang Guarantee, After Elliptic's Insights." Coindesk, May 15, 2025. https://www.coindesk.com/business/2025/05/15/telegram-shuts-down-largest-illicit-online-marketplace-after-elliptics-insights.

36 U.S. Department of the Treasury. "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia." Press release, October 14, 2025. https://home.treasury.gov/news/press-releases/sb0278.

37 Burgess, Matt, and Lily Hay Newman. "DOJ Issued Seizure Warrant to Starlink Over Satellite Internet Systems Used at Scam Compound." WIRED, November 14, 2025. https://www.wired.com/story/doj-issued-seizure-warrants-to-starlink-over-satellite-internet-systems-used-at-scam-compounds/.

38 Financial Crimes Enforcement Network. "Financial Trend Analysis Chinese Money Laundering Networks: 2020 – 2024 Threat Pattern & Trend Information." Washington, DC: FinCEN, 2025. https://www.fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf.

39 AML RightSource. "Scam States: The Cybercrime-Corruption Complex in Southeast Asia and the Collapse of Anti-Money Laundering Enforcement." September 2025. https://www.amlrightsource.com/resources/scam-states-the-cybercrime-corruption-complex-in-southeast-asia-and-the-collapse-of-anti-money-laundering-enforcement.

investments[40] and received tacit protection from state-aligned officials. In Laos, similar arrangements have allowed Golden Triangle SEZ leadership to maintain control of surrounding economic and enforcement levers.

In Myanmar, revenue from scam compounds directly fund several armed groups[41] participating in the civil war, with varying relationships to Chinese interests and the junta government. The Karen Border Guard Force and Karen National Union have each taken protection payments from Chinese transnational criminal organizations operating scam sites inside their respective zones. In exchange, these militias offer land, power, security, and insulation from enforcement; they've become revenue-sharing partners in the system.

These have resulted in a transnational infrastructure more than capable of operating under the current levels of pressure. Victims may be targeted in the U.S., lured from Manila, defrauded from Kayin State, and their assets laundered across Phnom Penh, Vientiane, and Shenzhen. Enforcement may hit individual sites, but such a decentralized system migrates, fragments, and rebuilds.

Mapping the Scam Economy: Key SEZs

Created with Datawrapper

GOLDEN TRIANGLE SEZ (LAOS)

Location	Northwestern Laos, bordering Thailand and Myanmar
Status	Nominal SEZ with extensive extraterritorial characteristics
Protection dynamics	Strong ties between developers, casino operators, and political elites
Operational significance	• Scam compounds embedded within casino and hospitality complexes • Victims frequently trafficked via Thailand and China before arrival
Why it matters	• Illustrates how SEZ legal exceptionalism facilitates cybercrime • High barriers to external inspection or sustained law-enforcement presence

The Golden Triangle SEZ in Laos, established in 2007 and controlled by the Dok Ngiew Group under Chinese businessman Zhao Wei, exemplifies how SEZs can become enclaves of criminal governance. Zhao Wei, sanctioned by the U.S. Treasury since 2018 for drug trafficking, human trafficking, money laundering, bribery, and wildlife trafficking, operates the Kings Romans Casino[42] as a central node for illicit activities. The SEZ functions as a quasi-autonomous zone where Laotian authorities exercise limited control, enabling a thriving criminal economy. The Golden Triangle SEZ has historically been a hot spot for narcotics trafficking,[43] particularly heroin produced in neighboring Myanmar, and a hub for wildlife trafficking,[44] including endangered species parts sold in contravention of the Convention on International Trade in Endangered Species of Wild Fauna and Flora. The zone also hosts extensive human trafficking

40 Global Initiative Against Transnational Organized Crime. Compound Crime: Cyber Scam Operations in Southeast Asia. Geneva: GI-TOC, May 2025. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

41 U.S.-China Economic and Security Review Commission. China's Exploitation of Scam Centers in Southeast Asia. Staff Research Report. Washington, DC: USCC, July 2025. https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf.

42 Global Initiative Against Transnational Organized Crime. Compound Crime: Cyber Scam Operations in Southeast Asia. Geneva: GI-TOC, May 2025. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

43 Ali Mc, "Abused, Exploited: How Two Africans Became Trapped in a Cyber-scam in Laos," Al Jazeera, May 31, 2025, https://www.aljazeera.com/features/2025/5/30/each-person-had-10-phones-trapped-in-a-cyber-scam-centre-in-laos.

44 García, Diana Paz, Vanda Felbab-Brown, and Vibha Bajji. "Chinese Crime and Geopolitics in 2024." Brookings, January 29, 2024. https://www.brookings.edu/articles/chinese-crime-and-geopolitics-in-2024/.

networks, with estimates suggesting up to 85,000 trafficked individuals[45] forced into labor in scam operations. The U.S. Institute of Peace estimates that scam centers in the Mekong region steal over $43.8 billion annually,[46] a significant portion of which flows through the Golden Triangle SEZ.

Despite international sanctions and diplomatic pressure, the Lao government has demonstrated limited capacity or will to dismantle the Golden Triangle SEZ's criminal operations. The zone's strategic location at the tri-border area of Laos, Myanmar, and Thailand provides porous borders and minimal oversight, facilitating the movement of drugs, people, and illicit capital. The Kings Romans Casino and associated high-rise buildings serve as command centers for scam operations, where workers face brutal conditions including beatings, electrocution, and starvation if they fail to meet quotas.

The Golden Triangle SEZ's criminal economy is sustained by a symbiotic relationship between Chinese organized crime syndicates, local militias, and corrupt officials.[47] This nexus exemplifies "criminal state-building," where illicit actors embed themselves within governance structures to maintain impunity and profit.

SHWE KOKKO AND KK PARK (MYANMAR)

Location	Myawaddy Township, Kayin State, directly across from Mae Sot, Thailand
Status	Operates in territory outside effective control of Myanmar's central government
Protection dynamics	Linked to ethnic armed organizations and local militias exercising de facto governance
Operational significance	• Large, purpose-built compounds combining worker housing, offices, and detention facilities • Reliance on cross-border electricity, internet connectivity, and logistics routed via Thailand
Why it matters	• Represents the convergence of civil war fragmentation and cybercrime infrastructure • Enforcement actions are constrained by sovereignty gaps and armed protection

Maxar satellite imagery of KK Park taken on January 17, 2024. (Satellite image (c) 2025 Maxar Technologies.)

Shwe Kokko and KK Park, located in Myanmar's eastern Kayin State near the Thai border, are infamous scam compounds operating under the protection of the Karen Border Guard Force,[48] a militia affiliated with the Myanmar military. These compounds have long served as hubs for cyber-scams, online gambling, and human trafficking, exploiting both local and foreign workers under coercive conditions.

The compounds' operations are characterized by a complex interplay of militia control, Chinese investment, and transnational criminal networks. The Karen Border Guard Force earns substantial revenue, approximately $192 million annually, from leasing land and providing security[49] to these scam operations. Despite Myanmar's military junta declaring a "zero tolerance" policy and conducting high-profile raids in late 2025, which resulted in over 2,000 arrests, the scam industry has proven resilient. Investigations reveal that scam

45 Global Initiative Against Transnational Organized Crime. "Compound Crime: Cyber Scam Operations in Southeast Asia." May 2025. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

46 United States Institute of Peace. "Transnational Organized Crime in Southeast Asia." 19 February, 2026. https://www.usip.org/programs/transnational-organized-crime-southeast-asia.

47 AML RightSource. "Scam States: The Cybercrime-Corruption Complex in Southeast Asia and the Collapse of Anti-Money Laundering Enforcement." September 2025. https://www.amlrightsource.com/resources/scam-states-the-cybercrime-corruption-complex-in-southeast-asia-and-the-collapse-of-anti-money-laundering-enforcement.

48 U.S. Department of the Treasury. "Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scam Operations." Press release, May 5, 2025. https://home.treasury.gov/news/press-releases/sb0129.

49 Global Initiative Against Transnational Organized Crime. Compound Crime: Cyber Scam Operations in Southeast Asia. Geneva: GI-TOC, May 2025. https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

operations quickly adapt by relocating workers and infrastructure to other compounds or across borders to Laos and Cambodia. The use of advanced technologies, such as Starlink satellite internet, enables these operations to maintain connectivity and evade detection. Phone data tracking has linked scam compounds directly to Myanmar military centers,[50] suggesting deep collusion between criminal actors and state officials.

Created with Datawrapper

SIHANOUKVILLE AND THMOR DA (CAMBODIA)

Location	Preah Sihanouk Province, southern Cambodia
Status	Former casino hub repurposed into dense scam-compound clusters
Protection dynamics	Links to local officials, security services, and politically connected developers
Operational significance	• High-rise buildings converted into scam offices and detention sites • Significant Chinese-language targeting and crypto-enabled laundering pipelines
Why it matters	• Demonstrates how urban redevelopment and foreign capital can mask criminal ecosystems • Periodic crackdowns have displaced, but not dismantled, operations

Sihanoukville[51] and Thmor Da in Cambodia have emerged as epicenters of forced labor[52] and human trafficking in the scam economy. These areas host numerous compounds where foreign nationals, primarily from China and Southeast Asia, are lured under false pretenses and subjected to brutal working conditions. Workers are forced into long hours of labor, physical abuse, and confinement, with reports of torture and deaths. The scam operations in these zones are linked to prominent Cambodian businessmen and politicians, including Ly Yong Phat, who has been sanctioned by the U.S. Treasury Department[53] for his role in human trafficking and forced labor. Ly Yong Phat's LYP Group and associated entities have been implicated in facilitating these crimes.

The Cambodian government's response has been inconsistent, with sporadic crackdowns, prompted in part, by the recent fighting with Thailand,[54] failing to dismantle the scam networks. Corruption and official complicity are pervasive, with reports indicating that police and other officials[55] are often involved in or profit from the trafficking and scam operations. The scam industry's profitability in Cambodia is staggering, with estimates suggesting annual revenues of $12.5 billion to $19 billion, accounting for up to 60% of Cambodia's formal GDP. The United Nations estimates[56] that 100,000 people had been trafficked into Cambodia's scam industry by late 2023.

50 PBS News. "Myanmar Has Declared a 'zero Tolerance' Policy for Cyberscams, but the Fraud Goes On," December 17, 2025. https://www.pbs.org/newshour/world/myanmar-has-declared-a-zero-tolerance-policy-for-cyberscams-but-the-fraud-goes-on.

51 Korea Times. "'It's Practically a Prison City': Inside Sihanoukville's Largest Scam Compound." October 17, 2025. https://www.koreatimes.co.kr/southkorea/law-crime/20251017/its-practically-a-prison-city-inside-sihanoukvilles-largest-scam-compound.

52 Global Initiative Against Transnational Organized Crime. "Compound Crime: Cyber Scam Operations in Southeast Asia." May 2025. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

53 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." Press release, September 12, 2024. https://home.treasury.gov/news/press-releases/jy2576.

54 Wee, Sui-Lee "Thailand, Attacking Cambodia, Says Its Target Is the Scam Industry" December 24, 2025. New York Times. https://www.nytimes.com/2025/12/24/world/asia/cambodia-scam-centers-refugees-thailand.html.

55 U.S.-China Economic and Security Review Commission. China's Exploitation of Scam Centers in Southeast Asia. Staff Research Report. Washington, DC: USCC, July 2025. https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf.

56 United Nations Office on Drugs and Crime. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

Created with Datawrapper

CLARK FREEPORT (PHILIPPINES)

Location	Former U.S. air base north of Manila
Status	Legal SEZ with prior concentration of POGO operations
Protection dynamics	Regulatory gaps during rapid expansion of offshore gambling
Operational significance	Scam and gambling operations shared infrastructure, labor pools, and payment channels Post-crackdown displacement rather than elimination of networks
Why it matters	• Shows how formal SEZs can be repurposed for cyber-enabled crime • Crackdowns pushed actors regionally rather than dismantling them

Clark Freeport in the Philippines is a significant hub for POGOs, which have become a legal cover for human trafficking, cybercrime, and scam operations. The Philippine Amusement and Gaming Corporation regulates POGOs, but enforcement is fragmented across multiple agencies, including the Clark Development Corporation,[57] police, and immigration authorities. This fragmentation has allowed criminal syndicates to exploit POGOs for illegal activities, including romance scams, cryptocurrency fraud, and human trafficking. The May 2023 raid on the Clark Sun Valley Hub[58] rescued over 1,100 trafficking victims, exposing the failure of intelligence and regulatory oversight. The Clark Development Corporation has since tightened visa processing and halted new POGO licenses, but illegal operations persist. POGOs have contributed to a rise in crimes such as tax evasion, kidnapping, prostitution, extortion, and murder in the Clark Freeport Zone. The involvement of foreign workers has led to widespread exploitation. The Philippine Senate has called for probes into POGO operations and the enforcement failures that enable these crimes.

Corruption and weak governance in the Philippines exacerbate the problem, with organized crime groups profiting from extortion, racketeering, and protection schemes. The scam operations in Clark Freeport are part of a broader regional criminal network, highlighting the need for coordinated enforcement and regulatory reforms.

Created with Datawrapper

OECUSSE DIGITAL TRADE ZONE (EAST TIMOR): EMERGING REPLICATION SITE

Location	Special Administrative Region of Oecusse-Ambeno (RAEOA), Timor-Leste, an exclave surrounded by Indonesian West Timor.
Status	Established as the Oecusse Digital Centre Free Trade Zone in December 2024 to attract investment and digital commerce.
Distinctive factors	Regulatory incentives and infrastructure aimed at digital commerce have created vulnerabilities exploited by transnational criminal networks. Development overlaps with blockchain payments (ODZT) and offshore company registries, raising concealment risks for illicit investment flows.
Why it matters	The early emergence of scam activity in a newly designated free trade zone demonstrates how novice zones can be targeted immediately as criminal "relocation sites," particularly when connected to broader organized networks operating in the region.

57 Malig, Jun A. "CIDG Raids POGO Firm in Tarlac, Rounds Up 850 Foreign, Filipino Employees." Inquirer.net. Philippine Daily Inquirer. 2 February, 2023. https://newsinfo.inquirer.net/1724643/cidg-raids-pogo-firm-in-tarlac-rounds-up-850-foreign-filipino-employees.

58 Malig, Jun A. "CIDG Raids POGO Firm in Tarlac, Rounds Up 850 Foreign, Filipino Employees." Inquirer.net. Philippine Daily Inquirer. 2 February, 2023. https://newsinfo.inquirer.net/1724643/cidg-raids-pogo-firm-in-tarlac-rounds-up-850-foreign-filipino-employees.

Emerging scam presence	In August 2025, authorities raided a suspected scam operation in the zone, detaining more than foreign nationals from Indonesia, Malaysia, and China for working without permits; evidence seized included SIM cards and Starlink devices, all indicators aligned with scam centers in Southeast Asia. UNODC reporting[59] links suspected activity to shell companies and organized networks previously seen in established hubs.

The Oecusse Digital Trade Zone in East Timor, established in December 2024, is rapidly emerging as a new hub[60] for scam operations. The United Nations Office on Drugs and Crime (UNODC) has warned that the zone's regulatory vulnerabilities and increased connectivity as East Timor joins ASEAN create an attractive environment for criminal networks. In late August 2025, police raided a suspected scam center[61] in Oecusse, detaining more than 30 foreigners working without permission. The zone has become a focal point for cyber-enabled scams, money laundering, and investment fraud, linked to notorious criminal groups including the 14K Triad. The UNODC estimates that these networks generate billions annually through scams and fraudulent investments.

Human Trafficking and Forced Criminality

The prevalence of forced criminality within Southeast Asia's scam ecosystems directly engages binding international and regional legal instruments, most notably the U.N. Palermo Protocol.[62] Under the protocol's definition of trafficking in persons, the recruitment, transportation, harboring, or receipt of individuals through deception, coercion, or abuse of power for the purpose of exploitation constitutes trafficking regardless of any apparent consent. Critically, exploitation under the protocol is not limited to sexual or physical labor but also encompasses forced participation in criminal activity when such participation is extracted through coercive means. This renders the routine classification of coerced scam operators as criminal perpetrators legally unsound.

The Palermo Protocol further establishes a non-punishment principle, obligating states to avoid penalizing trafficking victims for unlawful acts they were compelled to commit as a direct consequence of their exploitation. In the context of scam compounds, this principle is frequently breached when trafficked individuals are arrested, charged with fraud, or deported without trafficking assessments. A February 2023 complaint[63] report to ASEAN claims that Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Thailand, Singapore, and Vietnam have all been accused of violating the protocol. Such practices not only contravene international obligations but also risk state liability where patterns of misclassification are systematic rather than incidental.

At the regional level, ASEAN member states have committed to complementary standards through the ASEAN Convention Against Trafficking

59 United Nations Office on Drugs and Crime. Southeast Asia and the Pacific Organized Crime Threat Alert Strategic Infiltration of Vulnerable Jurisdictions through Criminal Foreign Direct Investments: the case of Timor-Leste. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, 2025. https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Alert_Strategic_infiltration_of_vulnerable_jurisdictions_through_criminal_foreign_direct_investments.pdf.

60 Al Jazeera. "UN Warns Online Scam Centres Hitting Southeast Asia, Moving to East Timor." September 12, 2025. https://www.aljazeera.com/news/2025/9/12/un-warns-online-scam-centres-hitting-southeast-asia-moving-to-east-timor.

61 Wu, Huizhong. "Scam Centers Are Spreading in East Timor, UN Report Says | AP News." AP News, September 12, 2025. https://apnews.com/article/unodc-scam-centers-east-timor-86da97b21652a5dd795ab7eabc403fea.

62 United Nations Office on Drugs and Crime. "United Nations Convention against Transnational Organized Crime and the Protocols Thereto: Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children." Accessed 2025. https://www.unodc.org/unodc/en/human-trafficking/protocol.html.

63 MigrantCare, Global Alliance Against Traffic in Women (GAATW), and Tenaganita. Complaint to the ASEAN Intergovernmental Commission on Human Rights (AICHR). February 2023. https://gaatw.org/advocacy/Complaint_to_AICHR_MigrantCare_GAATW_Tenaganita.Feb2023.pdf.

Workers are being released from a scam center based inside a casino in Sihanoukville, Cambodia, on January 18, 2026. (Magdalena Chodownik/ Anadolu via Getty Images)

in Persons (ACTIP),[64] which reinforces victim-centered approaches, explicitly calling for protection, assistance, and non-discriminatory treatment of trafficked persons, including foreign nationals. While ACTIP recognizes state sovereignty in law enforcement, it does not permit trafficking victims to be treated primarily as immigration violators or criminal suspects. The continued detention or deportation of individuals extracted from scam compounds without access to protection mechanisms therefore reflects an implementation gap rather than a legal vacuum.

The Ambiguity of Forced Criminality Is the Point

Human trafficking within Southeast Asia's scam ecosystems should not be understood as a secondary or incidental abuse arising from criminal activity. It is a structural mechanism that enables the industry to function at scale. Scam compounds across Myanmar, Cambodia, Laos, and the Philippines rely on trafficked labor to sustain high-volume, multishift operations that would otherwise be economically and operationally unviable. Forced criminality, wherein individuals are compelled under threat, violence, or confinement to participate in fraud, has become a defining feature of the regional cyber-scam economy. This structural reliance on coerced labor fundamentally blurs the distinction between victim and perpetrator. Individuals apprehended during raids are frequently found operating scam infrastructure, using multiple devices, engaging victims directly, or managing accounts while simultaneously meeting international legal definitions[65] of trafficking victims: "the recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception,

64 Association of Southeast Asian Nations. "ASEAN Convention Against Trafficking in Persons, Especially Women and Children." Accessed 2025. https://asean.org/asean-convention-against-trafficking-in-persons-especially-women-and-children/.

65 The Mekong Club. Exploiting Migration Channels: Trafficking for Forced Criminality in Southeast Asia. Updated December 2025. https://themekongclub.org/wp-content/uploads/2025/12/Exploiting-Migration-Channels-Trafficking-for-Forced-Criminality-in-Southeast-Asia.pdf.

Forced criminality, wherein individuals are compelled under threat, violence, or confinement to participate in fraud, has become a defining feature of the regional cyber-scam economy.

of the abuse of power or of a position of vulnerability."

This ambiguity has significant consequences for law enforcement and judicial processes. In multiple ASEAN jurisdictions, individuals removed from scam compounds have been detained, deported, or criminally charged for fraud-related offenses without adequate screening for trafficking indicators.[66] Such responses both violate victim-protection norms and actively undermine investigations. Coerced workers are unlikely to cooperate with authorities when they face punishment rather than protection. Moreover, rapid deportation often eliminates access to witnesses who possess critical knowledge of command structures, financial flows, and cross-border facilitation networks.

Forced criminality also complicates international cooperation. Scam operations routinely involve victims trafficked from outside the host country, including China, Vietnam, Thailand, the Philippines, and increasingly South Asia. This creates a jurisdictional confusion over responsibility for victim identification, repatriation, and legal accountability.

Without standardized regional protocols, enforcement actions risk shifting the humanitarian burden onto sending states while leaving organizers, financiers, and political enablers insulated from consequence. The persistence of these dynamics suggests that trafficking is both tolerated and functionally accommodated within existing enforcement frameworks.

From a policy perspective, the entrenchment of forced criminality exposes a critical mismatch between cybercrime suppression strategies and human rights obligations. Raids that focus narrowly on infrastructure disruption or arrest quotas may generate short-term visibility but leave underlying labor-coercion systems intact. In some cases, compound closures have resulted in victims being transferred directly into detention facilities[67] or informal custody arrangements, reinforcing these cycles of abuse, rather than dismantling them. These outcomes indicate that cyber-fraud enforcement divorced from trafficking-aware frameworks is both ineffective and counterproductive.

Addressing forced criminality within scam ecosystems therefore requires a shift in emphasis, wherein trafficked individuals are recognized as essential sources of intelligence and as protected persons under international law. Effective responses must integrate victim identification at the point of intervention, guarantee non-punitive treatment, and establish mechanisms for cross-border cooperation that prioritize both accountability and protection. Without such integration, regional efforts will continue to disrupt the visible symptoms of cyber-scam operations while leaving their human foundations, and their organizers, largely untouched.

Economic and Geopolitical Dimensions

The cyber-scam economy operating across Southeast Asia has reached a scale that is no longer marginal to regional political and economic systems. The UNODC estimates that cyber-enabled fraud originating in Southeast Asia generates between $18 billion and $37 billion annually, with assessments suggesting[68] the true figure may be higher once underreporting, laundering losses, and reinvestment cycles are considered. These revenues rival or exceed licit economic sectors in several border regions, creating powerful incentives for tolerance, protection, or active facilitation. Scam proceeds are routinely

66 The Mekong Club. Exploiting Migration Channels: Trafficking for Forced Criminality in Southeast Asia. Updated December 2025. https://themekongclub.org/wp-content/uploads/2025/12/Exploiting-Migration-Channels-Trafficking-for-Forced-Criminality-in-Southeast-Asia.pdf.

67 The Mekong Club. Exploiting Migration Channels: Trafficking for Forced Criminality in Southeast Asia. Updated December 2025. https://themekongclub.org/wp-content/uploads/2025/12/Exploiting-Migration-Channels-Trafficking-for-Forced-Criminality-in-Southeast-Asia.pdf.

68 Australian Institute of International Affairs. "Business as Usual? Chinese Organised Crime in Southeast Asia - Australian Institute of International Affairs," January 16, 2025. https://www.internationalaffairs.org.au/australianoutlook/business-as-usual-chinese-organised-crime-in-southeast-asia/.

reinvested into real estate developments, casinos, hotels, special economic zones, shell companies, or digital infrastructure, and this reinvestment embeds cyber-fraud into local patronage networks. These dynamics are most acute in conflict-affected areas, especially in Myanmar.

Along Myanmar's border regions, particularly those outside effective central government control, scam compounds have become integrated into wartime political economies. U.N. sources estimate that hundreds of thousands[69] of individuals have been trafficked or coerced into online criminal activity across the region, with Myanmar serving as a key hub due to fragmented sovereignty and the presence of armed actors. In several border areas, armed groups exercise de facto governance,[70] extracting rent or providing protection that enables scam operations to function with relative stability despite the ongoing civil war. While precise revenue flows are difficult to trace, the coexistence of scam infrastructure and armed conflict raises serious concerns about indirect conflict financing. Scam operators rely on territorial control, electricity, security, and logistics that are often mediated by militias or local power brokers. Even absent direct ownership, protection fees and revenue-sharing[71] arrangements risk channeling illicit profits into conflict economies, potentially prolonging instability. From a geopolitical standpoint, this blurs the line between cybercrime and conflict finance and complicates both sanctions regimes and peacebuilding strategies.

Beyond Myanmar, interstate dynamics continue to influence the scam ecosystem. Relations between Cambodia and Thailand have periodically

69 United Nations Office on Drugs and Crime. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

70 Global Initiative Against Transnational Organized Crime. "Compound Crime: Cyber Scam Operations in Southeast Asia." May 2025. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

71 Global Initiative Against Transnational Organized Crime. "Compound Crime: Cyber Scam Operations in Southeast Asia." May 2025. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

Thai military personnel inspect the O'Smach Casino complex, which housed a scam center, near the Thailand-Cambodia border on March 12, 2026 in Oddar Meanchey, Cambodia. (Getty Images)

strained over border management, labor migration, and security incidents, creating enforcement gaps that criminal networks exploit. In 2025, these tensions erupted multiple times into open fighting.[72] Scam operations frequently leverage these asymmetries: Victims are recruited in Thailand or abroad, trafficked through intermediary routes, and then exploited in Cambodian or border-adjacent facilities. Diplomatic frictions and jurisdictional disputes slow intelligence sharing and complicate joint investigations, allowing networks to adapt faster than state responses.

Despite public commitments to cooperation, outcomes have remained limited. Regional law-enforcement actions have resulted in the liberation of tens of thousands of victims and the arrest of thousands of low-level operators, yet UNODC reporting[73] indicates that the overall scale of scam activity has not meaningfully declined. Instead, operations relocate, fragment, or reconstitute under new legal entities. The pattern suggests that current cooperation mechanisms prioritize these visible disruptions over the sustained dismantling of financial and political enablers.

At the ASEAN level, coordination frameworks[74] acknowledge the transnational nature of the threat but remain constrained by consensus norms and uneven political will. Information-sharing is often bilateral and reactive, while disparities in enforcement intensity create opportunities for jurisdictional arbitrage. Scam networks exploit these differences by shifting infrastructure, personnel, and capital across borders while maintaining centralized control structures.[75] In effect, the regional governance environment favors mobility for criminals and fragmentation for enforcement.

China's Role: Source, Victim, and Selective Enforcer

China's involvement in Southeast Asia's cyber-scam crisis is multifaceted and complicated by the presence of Chinese criminal networks and its own state-level efforts to mitigate and respond to the problem. Neither dimension alone captures China's influence, as they shape both the drivers of the scam economy and the trajectory of regional cooperation. As well, despite some Chinese entities being the beneficiary of some of these operations, Beijing's own law enforcement data[76] show that thousands of Chinese nationals have been repatriated from scam compounds following bilateral operations.

Chinese transnational criminal organizations have played a central role in the development and expansion of scam compounds across Southeast Asia. Syndicates previously involved in illicit casinos and online gambling shifted into pig-butchering and other fraud schemes as Chinese domestic crackdowns[77] intensified in the 2010s. These groups have a presence in the scam centers in Myanmar, Cambodia, Laos, and other countries, employing technologies and money-movement tactics that drive tens of billions of dollars in illicit revenue annually.

A major example is She Zhijiang's Yatai New City project[78] in Myanmar's Shwe Kokko region, initially promoted as a smart city development but later

72 Center for Strategic and International Studies. "Fraud Frontlines: Scam Centers Caught in the Cambodia-Thailand Conflict." CSIS, 2025. https://www.csis.org/analysis/fraud-frontlines-scam-centers-caught-cambodia-thailand-conflict.

73 United Nations Office on Drugs and Crime. "Billion-dollar cyberfraud industry expands in Southeast Asia as criminals adopt new technologies." UNODC Regional Office for Southeast Asia and the Pacific, October 2024. https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html.

74 Southeast Asia Public Policy Institute. Towards an ASEAN Response to Scams. September 2025. https://seapublicpolicy.org/wp-content/uploads/2025/09/SEAPPI_Towards-an-ASEAN-response-to-scams_September-2025.pdf.

75 ISEAS – Yusof Ishak Institute. "Fraud with Danger: The Rise of Cyber Scams in Southeast Asia." ASEANFocus, Fulcrum. 16 December, 2024. https://fulcrum.sg/aseanfocus/fraud-with-danger-the-rise-of-cyber-scams-in-southeast-asia/.

76 Ewe, Koh. "Thousands of Chinese Lured Abroad and Forced to Be Scammers - Now Beijing Is Cracking Down," November 8, 2025. https://www.bbc.com/news/articles/c1lq95j1yp9o.

77 U.S.-China Economic and Security Review Commission. China's Exploitation of Scam Centers in Southeast Asia. Staff Research Report. Washington, DC: USCC, July 2025. https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf.

78 U.S. Department of the Treasury. "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams." Press release, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237.

converted into a platform for cyber-scams, trafficking, and forced labor under criminal syndicate control. She's activities are demonstrative of how Chinese criminal figures have embedded themselves within local economic projects and leveraged political ambiguity to sustain large scam operations. Other China-linked actors, such as figures associated with the Prince Group in Cambodia, have been sanctioned by U.S. and U.K. authorities[79] for alleged involvement in online fraud, human trafficking, and laundering large volumes of criminal proceeds, including bitcoin seizures valued in the billions.

While these criminal networks have origins that include Chinese actors, the Chinese state has also undertaken significant enforcement and response efforts. Publicly, Beijing has described overseas scam centers as threats to Chinese citizens' safety and diplomatic interests. China has coordinated repatriation flights for Chinese nationals rescued from scam compounds in Myanmar and Thailand, with over a thousand workers flown back for screening and assistance.[80]

China has also pursued legal action against transnational criminals linked to overseas scam operations. In late 2025, a Chinese court sentenced 11 individuals to death[81] over their roles in a syndicate accused of running extensive scam operations near Myanmar's border that was valued at more than $1.4 billion and tied to forced labor and violent suppression of workers.

These actions demonstrate that Chinese authorities view cross-border scam networks as a domestic law enforcement priority, particularly when Chinese citizens are victims or stakeholders. However, these official efforts are uneven and often reactive. They focus on repatriation and prosecution after crises, rather than a sustained disruption of criminal syndicates far from Chinese jurisdiction.

China's engagement with Southeast Asian states on the scam crisis is also influenced by the country's broader geopolitical considerations. Beijing has publicly urged ASEAN countries to treat online scam networks as shared security threats and has participated in joint initiatives. For example, China and Thailand agreed to establish a joint coordination center[82] in Bangkok (with a branch near the Myanmar border) to combat telecom and online fraud networks staffing scam compounds with trafficked workers. At the same time, China's deployment of these cooperative mechanisms can function as a lever of influence. Its security and policing cooperation is tied to concerns about the reputational and social impact of scams on Chinese tourists and citizens, reinforcing China's role as a regional security partner, even as some observers argue that Beijing has been slow to crack down on groups that serve economic or political interests.

This interaction between criminal actors with ethnic or operational ties to China and state-level cooperation and enforcement efforts creates both opportunities and challenges for regional responses. It complicates how Southeast Asian governments view Chinese involvement as both the source of the problem and part of the solution. Effective policies must navigate this duality by supporting sustained, institutionalized cooperation while guaranteeing that enforcement actions target the underlying structures of transnational criminal networks, rather than only their symptomatic actors.

79 U.S.-China Economic and Security Review Commission. China's Exploitation of Scam Centers in Southeast Asia. Staff Research Report. Washington, DC: USCC, July 2025. https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf.

80 Skulpichetrat, Jutarat, and Grant Peck. "China Begins Repatriation From Thailand of More Than 1,000 Online Scam Workers Rescued From Myanmar | AP News." AP News, February 20, 2025. https://apnews.com/article/myanmar-online-scam-centers-myawaddy-trafficking-china-thailand-9fce90b60eb8cf5a42569f0e7ec865f6.

81 The Guardian. "China Court Sentences 11 People to Death over Alleged Role in Family-Run Myanmar Scam Operations." September 30, 2025. https://www.theguardian.com/world/2025/sep/30/china-court-sentences-11-people-to-death-over-alleged-role-in-family-run-myanmar-scam-operations.

82 Reuters. "Thailand, China Set Up Coordination Centre to Combat Scam Call Networks." January 24, 2025. https://www.reuters.com/world/asia-pacific/thailand-china-set-up-coordination-centre-combat-scam-call-networks-2025-01-24/.

Cyberscams in Numbers

300,000+ VICTIMS

$64B ANNUAL GLOBAL PROFITS

74% OF SCAM COMPOUNDS BASED IN THE MEKONG REGION

Source: OHCR

Countermeasures and Systemic Gaps

Regional and international countermeasures targeting Southeast Asia's cyber-scam ecosystem have expanded markedly since 2022, but they remain structurally misaligned with the political economy sustaining these operations. While ASEAN member states and external partners have increased cooperation, enforcement actions continue to prioritize visible disruption over systemic dismantling, allowing scam networks to adapt, relocate, and persist.

At the ASEAN level, responses are formally anchored in existing transnational crime and trafficking frameworks, most notably ACTIP.[83] These instruments establish shared commitments to victim protection, information exchange, and cooperation, but they lack binding enforcement authority, centralized investigative capacity, or mechanisms to compel compliance. Because of this, ASEAN action has largely taken the form of policy coordination,[84] joint statements, and ad hoc task forces rather than sustained regional investigations or prosecutions. Structural constraints within ASEAN further limit its effectiveness. Consensus-based decision-making slows response times, while non-interference norms discourage scrutiny of politically sensitive special economic zones or elite-linked developments. Implementation varies widely[85] across member states, particularly in border regions where scam operations are most entrenched. UNODC assessments consistently note that while ASEAN forums increasingly recognize cyber-enabled fraud as a regional security threat, operational outcomes remain fragmented, reactive, and nationally siloed.

ASEAN+ partners bring substantial capabilities to the counter-scam effort, but these are unevenly integrated into regional frameworks. China plays the most operationally visible role. Beijing has coordinated large-scale repatriations of Chinese nationals trafficked into scam compounds, conducted joint policing actions with Thailand and Myanmar authorities, and established bilateral coordination mechanisms such as the China-Thailand anti-fraud center[86] announced in 2025. These actions have produced concrete results such as rescues, arrests, and prosecutions, but they are selective in scope, prioritizing cases involving Chinese citizens and domestic reputational risk. They do not systematically address non-Chinese victims, financial facilitators, or host-country political protection networks, and enforcement pressure has frequently displaced scam activity rather than reduced it.

Western partners, including the United States, the European Union, and Australia, have focused on complementary but indirect tools. These include targeted sanctions against individuals and entities linked to cyber-fraud and trafficking, capacity-building for cybercrime units and financial intelligence agencies, and cooperation on cryptocurrency tracing and anti-money-laundering enforcement. While these measures strengthen technical capacity, they depend on domestic political will and legal follow-through in jurisdictions where scam revenues are intertwined with local economic and patronage systems. UNODC reporting highlights that financial-investigation assistance is routinely undercut when authorities lack incentives to pursue politically connected actors.

83 Association of Southeast Asian Nations. "ASEAN Convention Against Trafficking in Persons, Especially Women and Children." https://asean.org/asean-convention-against-trafficking-in-persons-especially-women-and-children/.

84 Southeast Asia Public Policy Institute. Towards an ASEAN Response to Scams. September 2025. https://seapublicpolicy.org/wp-content/uploads/2025/09/SEAPPI_Towards-an-ASEAN-response-to-scams_September-2025.pdf.

85 United Nations : UNODC Regional Office for Southeast Asia and the Pacific. "Cyberfraud in the Mekong Reaches Inflection Point, UNODC Reveals," 21 April, 2025. https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html.

86 UN News. "UNODC Joins Regional Crime Fighters to Tackle Scams and Human Trafficking in SE Asia," September 26, 2023. https://news.un.org/en/story/2023/09/1141492.

Systemic Gaps

Across ASEAN+, three systemic gaps exist. First, enforcement incentives remain misaligned. Operations overwhelmingly target compounds, trafficked workers, and low-level facilitators, while developers, financiers, protection providers, and political enablers remain largely insulated. In regions where scam revenues sustain construction booms, local employment, or armed actors, enforcement directly competes with entrenched economic interests.

Second, victim protection remains inconsistently integrated into enforcement. Raids and shutdowns frequently fail to incorporate trafficking-aware procedures, resulting in the detention or deportation of coerced workers. This violates international obligations, undermines intelligence collection, and discourages cooperation from victims who possess critical knowledge of scam networks. OHCHR and UNODC reporting consistently identify this pattern as a recurring failure across the region.

Third, jurisdictional fragmentation continues to favor criminal mobility. Scam networks operate transnationally, but investigations remain overwhelmingly national or, at most, bilateral. There is no standing regional mechanism for joint financial investigations, shared evidence repositories, or coordinated prosecutions. Criminal organizations exploit this fragmentation by shifting infrastructure, personnel, and capital across borders while maintaining centralized command and financial control.

Taken together, these gaps produce a countermeasure environment characterized by activity without resolution. ASEAN frameworks provide legitimacy but lack coercive power. ASEAN+ partners contribute capacity, but they act selectively or externally. The result is a system that absorbs enforcement pressure without collapsing, and enables scam networks to relocate, rebrand, and regenerate.

Absent a shift toward institutionalized regional investigations, financial-centric enforcement that targets enablers rather than operators, and politically insulated victim-protection mechanisms, countermeasures will continue to suppress symptoms while leaving the underlying political economy of cyber-enabled fraud intact.

POLICY RECOMMENDATIONS

The United States cannot resolve Southeast Asia's cyber-scam crisis unilaterally, but it can meaningfully reshape the incentive environment in which scam ecosystems operate. Given the transnational, politically embedded nature of these operations, an effective U.S. strategy should prioritize financial disruption, institutional leverage, and victim-centered enforcement rather than compound-by-compound takedowns. The objective would be to substantially increase systemic pressure on enablers

1 REFRAME CYBER-SCAM OPERATIONS AS A HYBRID SECURITY THREAT

The U.S. should formally treat large-scale scam ecosystems as a hybrid threat encompassing transnational organized crime, human trafficking, illicit finance, and, where applicable, conflict financing. This framing would justify sustained interagency prioritization rather than ad hoc responses driven by individual cases or media attention.

Practically, this means elevating Southeast Asian scam networks within U.S. strategic documents on transnational crime and integrating them into Indo-Pacific security dialogues. Doing so would align cybercrime policy with broader U.S. objectives on human rights, regional stability, and economic integrity, rather than isolating scams as a consumer-protection issue.

2 SHIFT THE CENTER OF GRAVITY TO FINANCIAL AND ENABLER TARGETING

U.S. efforts should move decisively away from an operator-centric enforcement model toward enabler-centric disruption.

This includes:

- Expanding Treasury-led sanctions against developers, financiers, shell companies, and logistics providers linked to scam ecosystems using the Global Magnitsky Act, which authorizes the U.S. government to sanction foreign individuals responsible for human rights abuses or significant corruption.
- Prioritizing financial intelligence cooperation focused on real estate laundering, casino-linked cash flows, and crypto-fiat conversion points rather than individual scam wallets.
- Supporting partner-country investigations into commercial infrastructure such as telecom providers, hosting services, and payment processors, which are all used systematically by scam networks.

UNODC and U.S.[87] government reporting consistently show that scam operations survive enforcement by replacing labor and infrastructure but struggle when capital access and elite protection are constrained. Targeting these choke points offers the highest leverage at lowest operational cost.

Recent U.S. legal momentum suggests movement in this direction. The Office of Foreign Assets Control's action [88]against the Prince Group and Huione Group is an important step. As well, the U.S. Treasury Department has targeted Funnull Technology for selling bulk IP infrastructure to cybercriminals, and the Karen National Army for compound protection. The pattern across these actions show that there is a shift toward enabler-centric logic. The challenge now is sustaining and deepening it, rather than treating each action as discrete.

3 EMBED VICTIM PROTECTION AS AN INTELLIGENCE AND ENFORCEMENT ASSET

The U.S. should explicitly promote non-punitive, trafficking-aware enforcement models as a core component of counter-scam strategy. It can't be framed solely a human rights issue, and should be appreciated as an intelligence multiplier.

Policy tools include:

- Conditioning certain forms of U.S. law-enforcement assistance on the adoption of victim screening and protection protocols consistent with the Palermo Protocol.
- Supporting regional victim-identification training tied to evidence preservation and witness cooperation, rather than rapid deportation.
- Funding NGO and international-organization programs that facilitate safe cooperation pathways for trafficking victims willing to provide testimony.

Evidence from prior interventions indicates that coerced workers possess critical insight into command hierarchies, financial flows, and relocation patterns. This is insight that is lost when victims are treated as offenders.

4 USE ASEAN+ MECHANISMS WITHOUT FORCING ASEAN CENTRALITY

The U.S. should continue engaging ASEAN as a normative anchor while accepting its institutional limitations. Rather than pushing for new ASEAN-wide enforcement bodies, which are unlikely to materialize, the U.S. should focus on modular, opt-in cooperation among willing states.

87 UN News. "UNODC Joins Regional Crime Fighters to Tackle Scams and Human Trafficking in SE Asia," September 26, 2023. https://news.un.org/en/story/2023/09/1141492.

88 U.S. Treasury Department. "U.S. And U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia," February 13, 2026. https://home.treasury.gov/news/press-releases/sb0278.

This includes:

- Supporting minilateral investigative coalitions among high-capacity partners (Thailand, Singapore, Philippines) that can later be expanded.
- Leveraging ASEAN+ platforms to standardize financial and evidentiary cooperation, even where policing remains national.
- Coordinating discreetly, but deliberately, with China on cases of shared interest, while avoiding overdependence on Chinese-led enforcement priorities.

This approach preserves ASEAN legitimacy without allowing consensus constraints to paralyze action.

5 INTEGRATE SCAM ECOSYSTEMS INTO U.S. CONFLICT AND STABILITY PLANNING

In areas such as Myanmar's border regions, scam operations intersect directly with armed conflict and fragmented sovereignty. The U.S. should incorporate cyber-scam economies into its conflict analysis and sanctions planning and recognize their role in sustaining local power structures.

Where appropriate, this includes:

- Assessing whether scam-derived revenue contributes indirectly to armed actors or conflict persistence
- Aligning counter-scam sanctions with existing human rights and conflict-related measures
- Avoiding enforcement actions that inadvertently strengthen armed intermediaries by eliminating rival revenue streams without addressing protection arrangements.

Treating scam ecosystems as part of broader war-crime economies improves coherence across U.S. policy domains.

Recent shifts in U.S. policy have also shown a somewhat greater willingness to directly sanction conflict-entangled entities. This precedent supports integrating similar analysis into future sanctions planning across Myanmar's fragmented armed landscape.

Strategic End State

The United States shouldn't necessarily aim for the eradication of cyber-scam operations, a near-impossible task under current conditions, but it can push for a durable reduction in scale, profitability, and political insulation. Success should be measured by rising operational costs for enablers, declining impunity for financiers, improved victim outcomes, and increased friction across borders.

Absent such a clear strategy, the current level of U.S. engagement risks reinforcing the current pattern of high-visibility enforcement activity that generates headlines but leaves the underlying political economy of cyber-enabled fraud largely intact.

AUTHOR

Mark Bruno is a cybersecurity specialist and former U.S. Army combat medic and public affairs representative. He holds a master of science in cybersecurity and is currently completing a master of arts in International Relations and Security Studies at Webster University Leiden. His work explores the intersection of emerging technologies and global conflict, with his recent research critically examining growing surveillance states. He also brings a background in digital communications, with experience in journalism, media production, and strategic communication.

NEW LINES INSTITUTE
FOR STRATEGY AND POLICY

Contact

For media inquiries, email
media@newlinesinstitute.org

To learn more about New Lines' publication process, email
submissions@newlinesinstitute.org

For other inquiries, send an email to
info@newlinesinstitute.org

A: 1660 L St. NW, Ste. 450
Washington, D.C., 20036

P: (202) 800-7302