THE SELECT COMMITTEE ON THE
STRATEGIC COMPETITION BETWEEN
THE UNITED STATES AND
THE CHINESE COMMUNIST PARTY

CRIME, *CORRUPTION*, and *POWER*

CCP-Linked Transnational Crime and the Rise of a Distributed Threat to U.S. National Security

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A Human Entry Point into a Strategic Threat

Struggling to find work amid the economic downturn following the COVID-19 pandemic, Maya* believed she had found a promising job opportunity overseas. Instead, she was recruited to Cambodia and trafficked by transnational criminal organizations (TCOs) with origins in the People's Republic of China (PRC). She found herself trapped inside a fortified compound protected by corrupt local elites and forced under threat of physical and sexual violence to defraud Americans through online investment scams.

Maya's experience may sound extreme, but it is by no means an outlier: hundreds of thousands of people have been deceptively drawn into industrialized scam operations across Southeast Asia where they are trafficked for the purpose of forced criminality, while Americans lose at least $10 billion each year to PRC-origin scam networks across the region.[1]

Organized crime in the Indo-Pacific has entered a historic new phase. Once-fragmented enterprises involved in online gambling, cyber fraud, human trafficking, forced criminality, and money laundering have converged into transnational networks built for scale, speed, and profit. These networks unlawfully move people and capital across borders with limited friction, exploit PRC-facing financial channels, and adapt rapidly to pressure. The result is not a series of isolated criminal schemes, but a durable regional criminal economy with direct and material consequences for American citizens, companies, allies, partners, and national security.

The urgency to act now stems from both the staggering scale of current losses and the likelihood these operations will continue to grow. U.S. government assessments have identified cyber-enabled investment fraud, often referred to by scammers as "pig butchering," as among the fastest-growing and most financially devastating forms of cybercrime targeting Americans.[2] Fraud victims frequently lose retirement savings, home equity, or family assets after months of sustained manipulation. Many are subsequently re-targeted by secondary fraud schemes often impersonating law enforcement or other entities positioned to help recover stolen assets. Beyond financial injuries, these harms are deeply psychological and emotional as well.

Prior congressional and executive branch efforts have elevated awareness of scam centers, human trafficking, and cyber fraud. What has historically remained unexamined is how these activities fit within a broader pattern of convergent transnational organized crime with links to the Chinese Communist Party (CCP); how different forms of CCP linkages can be distinguished analytically; and which tools are best suited to counter a threat that is distributed, adaptive, and deeply embedded within regional political economies.

*Maya is a pseudonym for one of the human trafficking survivors interviewed as part of this investigation.

[1] U.S. Department of the Treasury, "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams," press release, September 17, 2025.

[2] U.S. Department of Justice, "Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans," press release, April 23, 2026.

A Distributed Threat

According to evidence reviewed by the Select Committee, the scam industry and its underpinning criminal networks are not directed by Beijing in a grand conspiracy. Rather, our investigation identifies "CCP-linked" transnational criminal organizations as a more complex and durable threat: a regional system in which criminal networks, selective PRC enforcement, host-state corruption, illicit finance, forced labor, and private sector infrastructure reinforce one another. This system causes immense harm to foreign populations, including U.S. citizens, while embedding itself within local political economies and governance structures.

While its mechanisms differ from traditional military or territorial threats, the cumulative effects on governance, financial integrity, regional stability, and coercive leverage are comparable in scale and, in some cases, harder to counter. Treating this threat as peripheral or purely a law enforcement problem understates both its persistence and its strategic consequences.

The erosion of the rule of law carries direct security consequences for the United States, including its strategic competition with the CCP. When criminal networks entrench themselves politically, partner states struggle to implement sanctions, regulate infrastructure, or sustain security cooperation. These weaknesses create exploitable gaps in the regional security system.

Case Studies and Strategic Patterns

The Select Committee investigation examined a selected set of cases rather than a comprehensive survey of every jurisdiction affected. Cambodia and Burma serve as the primary cases because they represent the most mature and strategically consequential forms of CCP-linked criminal entrenchment. The Philippines, Pacific Island states, and emerging frontiers cases illustrate how this entrenchment varies, spreads, and can be reversed across different governance environments. Across these cases, this report finds:

1. When pressure rises inside China or in existing hubs, criminal networks and their harms are pushed outward. As these networks have matured and migrated across Southeast Asia, Americans have become primary victims of a transnational fraud economy that simultaneously undermines core U.S. national security interests.

2. Protection markets and political insulation reduce operational risk for CCP-linked criminal networks. The form of complicity varies by case: party ties to criminal actors, politically selective PRC enforcement, China-facing financial rails, host-state corruption, and state-adjacent legitimacy systems all play different roles.

3. Infrastructure designed for legitimate use can become criminally useful when oversight lags. Casinos, real estate, special economic zones, telecommunications networks, and online platforms can provide the physical, digital, and jurisdictional architecture through which scam networks scale, conceal operations, and adapt to enforcement pressure.

4. Shadow financial systems – including underground banking, crypto brokers, shell companies, and identity arbitrage – provide the connective tissue that allows proceeds to move across borders for exploitation by other hostile or sanctioned networks. These systems allow

illicit proceeds to be laundered, reinvested, and repurposed across jurisdictions, linking Southeast Asia-based scam networks to broader risks.

Implications for Congress

First and foremost, this report recommends that the CCP-linked transnational fraud ecosystem be treated as its own high-priority national security category. It overlaps with organized crime, cybercrime, corruption, human trafficking, human rights abuses, democratic backsliding, illicit finance, and great power competition, but it cannot be reduced to any one of them alone. Its strategic significance lies precisely in that convergence.

Additionally, despite varying degrees of PRC state complicity with the industry, we *do not* recommend complete disengagement from Beijing on this issue. The United States can and should welcome verifiable bilateral cooperation where it produces concrete gains for U.S. citizens, trafficking victims, or partner governments. But tactical cooperation – particularly when strategically deployed in the lead-up to major convenings – should not be interpreted with undue optimism.[3] The evidence suggests that Beijing's incentives remain highly selective and misaligned. A durable U.S. response must therefore combine law enforcement, financial pressure, diplomacy, governance support, civil society support, private sector coordination, allied action, and independent intelligence collection. Critically, this should be done with the broad coalition of actors whose interests are aligned on this issue.

Distributed threats require distributed resilience. Anything narrower will leave Americans exposed, U.S. partners and allies vulnerable, and a global system of crime, corruption, and coercion intact.

The United States Government should:

1. Pass bipartisan scam center legislation, specifically the Dismantle Foreign Scam Syndicates Act;
2. Strengthen the statutory basis for sustained interagency coordination;
3. Increase pressure on foreign CCP-linked protection networks;
4. Support governance resilience in vulnerable states;
5. Coordinate with partners and allies to prevent criminal displacement;
6. Engage private sector infrastructure as a national-security partner; and
7. Pursue verifiable, tactical cooperation with the PRC where it advances U.S. interests, victim protection, or partner-government capacity.

[3] Laura Zhou, "US and China in 'Unprecedented' Cooperation Against Scam Centres in Dubai," *South China Morning Post*, May 13, 2026, https://www.scmp.com/news/china/diplomacy/article/3353389/us-and-china-unprecedented-cooperation-against-scam-centres-dubai.

Crime, Corruption, and Power

CCP-Linked Transnational Crime and the Rise of a Distributed Threat to U.S. National Security

PART I. BACKGROUND AND INTRODUCTION

On January 7, 2026, Chinese authorities took custody of Chen Zhi – the 38-year-old Fujian-born, Cambodia-naturalized founder and chairman of Prince Holding Group, a Cambodia-based conglomerate that U.S. prosecutors describe as the hub of a massive global scam, illegal gambling, and illicit finance network.[4] Chinese and Cambodian authorities framed his detention as routine bilateral law enforcement cooperation, following a months-long joint investigation.[5] The timing and circumstances, however, warrant closer examination.

Chen Zhi's relationship to the Cambodian government was unambiguous. In his ten years as a naturalized citizen, he had rapidly risen to become a close personal friend of strongman Hun Sen and was a named cabinet-level advisor to his dynastically appointed son, Hun Manet. Over the same span, Prince Holding Group had emerged from obscurity into one of the most visible brand presences in the entire country, while expanding regionally.

Interviews with PRC officials dating back years suggest that different parts of the Chinese state had conflicting aims relative to Chen and his Prince Holding Group. On one hand, Chinese officials reported seeking Chen's extradition years earlier, but those efforts appear to have been constrained by Beijing's desire to maintain strategic equilibrium with a criminalized regime in Phnom Penh.[6] Conversely, former Chinese intelligence officers have gone on-record stating that they were actually working collaboratively *with* Prince to achieve strategic aims of the Chinese state in Cambodia.[7] Neither stance is fully verifiable; however, both can be simultaneously true.

By the time of his extradition, international scrutiny of Chen's activities had been mounting for years. Since at least 2019, but escalating significantly in 2024 and 2025, independent journalists, researchers, and civil society organizations widely documented Prince Holding Group's role in large-scale scam operations, human trafficking, and illicit finance across Southeast Asia and beyond, alongside Chen's extraordinary political access within Cambodia.[8]
On October 14, 2025, U.S. authorities filed the largest forfeiture action in history – announcing the seizure of $15 billion in bitcoin from unhosted wallets in Chen's possession. The forfeiture was accompanied by a federal indictment and joint U.S.-U.K. sanctions, targeting 117 individuals in Prince's network, alleging

---

[4] Grant Peck, "Alleged Scam Kingpin Chen Zhi Arrested in Cambodia," *Associated Press*, January 7, 2026, https://apnews.com/article/cambodia-scam-chen-zhi-prince-group-china-b32da55af90841d6b2b95cc6334f3fa7.
[5] "Prince Holding Group Founder Chen Zhi Arrested, Extradited to China: Interior Ministry," Khmer Times, January 8, 2026, https://www.khmertimeskh.com/501823113/prince-holding-group-founder-chen-zhi-arrested-extradited-to-china-interior-ministry/.
[6] Jacob Sims, Policies and Patterns: Transnational Crime in Cambodia as a Global Security Threat (Humanity Research Consultancy / USAID, 2025).
[7] Jack A. Davies, follow-on investigative reporting on Cambodia's scam economy and enforcement dynamics, 2024–2026.
[8] Jack A. Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?" Radio Free Asia, February 5, 2024.

forced labor, transnational fraud, money laundering, and the maintenance of operational nodes inside the United States.[9] [10] [11]

Seen against this chronology, Chen's removal by Chinese authorities cannot be understood simply as an isolated law enforcement exercise. It reflected a moment when continued patterns of inaction had become strategically untenable – both for Beijing and its partner in Phnom Penh. As the prospect of U.S. or allied action grew more likely, and the costs of inaction rose, plausible deniability narrowed. At that point, action by Beijing became unavoidable.

From Criminal Capital to Political Power

The dynamics that led to Chen Zhi's rise and eventual fall are illustrative of the broader transformation underway in Indo-Pacific organized crime. His activities in China during the early 2010s involved online gaming and gambling fraud that generated significant criminal proceeds and legal exposure. Chen then emerged several years later in Cambodia as a major investor and public figure.[12]

Yet, this checkered past did not stop a central Chinese SOE subsidiary (China Construction Fourth Engineering Division) from constructing major Prince Group assets in Cambodia, including numerous buildings now known to have been used to scam Americans using forced labor.[13] For further detail on this relationship, see the Appendix.

Whether his relocation from China to Cambodia reflected flight from, facilitation by, or tolerance by Chinese authorities is not definitively known. What is clear is this: his prior activities gave the Chinese state enduring leverage over him; the PRC has repeatedly demonstrated its ability to pressure other states to disenfranchise or extradite its nationals abroad when sufficiently motivated; and his prominence in Cambodia made him more useful there than in a Chinese prison, until it did not.

In Cambodia, Chen did not merely invest and build; he consolidated power. Over just a few years, he rose to a cabinet-level adviser to both the former and current prime ministers, obtained Cambodian citizenship and a diplomatic passport**,** and led what became the most visible and ubiquitous corporate brand in the country**,** spanning real estate, infrastructure, casinos, hotels, and digital services, rapidly becoming a leading patron to the ruling Cambodian People's Party and its strongman. Former Cambodian Prime Minister Hun Sen publicly referred to Chen using a familial nickname normally reserved for his own children, a symbolic gesture widely interpreted as signaling historically exceptional political favor and trust.[14] In Cambodia as elsewhere in the region where China exerts significant influence, this level of political integration affords extraordinary insulation from scrutiny or enforcement.

---

[9] U.S. Department of Justice, "Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes," press release, October 14, 2025, https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged.

[10] 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.

[11] *United States v. Chen Zhi*, No. 1:25-cr-00312-RPK (E.D.N.Y. Oct. 8, 2025) (indictment unsealed Oct. 14, 2025), https://www.justice.gov/usao-edny/media/1416286/dl.

[12] Helen Regan, "Cambodia Scams: The Rise and Fall of Chen Zhi and the Prince Group," CNN, October 24, 2025.

[13] 中国建筑第四工程局, "柬埔寨西港太子IT大厦项目成功中标," March 2018, http://4b1.cscec.com/xwzx/qyyw/201803/3155295.html

[14] Yan Huang, "The Rise and Fall of Chen Zhi," Cambodia: Rain and Dust, January 9, 2026.

Criminal operations allegedly flourished under this protection, with scam compounds, online gambling, underground banking, and illicit finance embedded within development projects.

Opaque State Relationships and Persistent Non-Action

Chen's well-documented relationship with the Cambodian state is matched by long-standing questions about his relationship with the Chinese state. For more than a decade, despite credible reporting on his criminal activities and the PRC's demonstrated ability to secure the extradition of its nationals abroad, Chen remained untouched by Chinese law enforcement. Various independent (albeit difficult to fully substantiate) reports also allege that Prince Group served as a vehicle for Chinese influence-building in Cambodia, including above-noted claims by a defected Chinese intelligence officer that he had been formally placed within the company to advance CCP objectives.[15]

Analysts have described similar patterns across the region, in which prominent scam-linked actors face prolonged tolerance followed by selective intervention once they become diplomatically costly or politically exposed.[16][17] Chen's January 2026 extradition to China fits that pattern.

By 2019, scrutiny of Chen's activities began to intensify. Investigative reporting eventually documented the scale of scam operations and trafficking linked to Cambodia's casino and online gambling sector. Over the next several years, that scrutiny escalated, reaching a crescendo in October 2025 with a wave of law enforcement, sanctions, and regulatory actions cascading across the United States, Europe, and Asia. By December 2025, Chen's global Prince network faced a narrowing funnel of exposure and his political enablers in Cambodia were significantly weakened by a losing conflict with Thailand and an eroded international reputation. Together, these factors shifted the calculus that had long protected him. His January 2026 arrest was *likely* precipitated by this dynamic and his extradition to China now *certainly* implies that any evidence he might hold will remain permanently out of more neutral and transparent court systems.

A Distributed Ecosystem, Not a Centralized Conspiracy

While Chen Zhi is, by some estimates, one of the wealthiest, most transnational, and most politically well-connected criminals in history, he is not a one-off. Rather, he is an exemplar of a broader regional system in which crime, corruption, and coercion mutually reinforce one another under permissive governance conditions. These conditions – characteristic of the CCP's governance model and its tightening regional hegemony – do not require centralized orchestration or a top-down strategy to shape outcomes. They operate through norms of selective enforcement and political protection that inherently shield criminal activity from accountability, in many documented instances with varying degrees of knowing complicity by CCP-linked elites or formal state apparatus.[18]

---

[15] Gaétan Pouliot, "A Chinese Dissident Died Suddenly in B.C. This Ex-Spy Who Snooped on Him Says It May Not Have Been an Accident," CBC News / Radio-Canada, December 8, 2025, https://www.cbc.ca/news/world/chinese-spy-speaks-out-enquete-radio-canada-9.7003661.

[16] United States Institute for Peace (USIP), Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security, United States Institute of Peace Senior Study Group Final Report (May 2024), https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf

[17] Bertil Lintner, "Untangling Scam Kingpins' Ties to the Chinese Government," *The Irrawaddy*, February 2026.

[18] USIP, Transnational Crime in Southeast Asia (2024).

While this corrupted environment arises from long-standing CCP governance patterns, it does not always uniformly serve Chinese interests. Indeed, it is difficult to look at Southeast Asia's scamdemic without seeing that Chinese citizens were its first and biggest losers – as victims of both trafficking and scams. Moreover, the Chinese state's role has been and remains ambiguous, acting as both a selective disruptor and opportunistic enabler, sometimes in the same action. A 2024 senior study published by the U.S. Institute of Peace called the relationship between the Chinese state and the syndicates "a confusing complex of mixed incentives and mutual opportunity" and little has emerged in the last two years to fundamentally shift that assessment.

Accordingly, this report does not proceed from the assumption of a centralized CCP conspiracy directing organized crime as an explicit tool of state policy. Rather, it advances a more grounded claim, that: ***a distributed regional ecosystem has emerged in which PRC-origin TCOs, state-linked actors, and PRC-influenced governance environments marked by crime, corruption, and coercion reinforce one another to the significant detriment of U.S. citizens, regional partners, and U.S. values-based and national security-related foreign policy objectives.*** Within this ecosystem, while linkages between criminals and CCP elites or state entities are documented, criminal activity appears to be enabled less by a central command node in Beijing than by consistent regional patterns of tolerance, facilitation, and exploitation that reduce risk and allow illicit networks to entrench across borders.[19]

Strategic Significance of a Distributed Threat

The distributed nature of this threat helps explain its durability. Because the system operates through market incentives, corrupt protection networks, and portable financial and digital infrastructure, it can absorb enforcement pressure and reconstitute across borders. That makes it harder to counter than a single organization, compound, or command structure.

These dynamics are most visible in countries such as Cambodia and Burma**,** where criminal, coercive, and corrupt practices have combined with local regime-aligned interests (a conflict economy in Burma and a criminalized stability in Cambodia) to produce highly concentrated and durable hubs of illicit activity.[20] [21] These cases illustrate how state-abetted criminal ecosystems, once established, can reproduce themselves, attract transnational networks, and function as alternative systems of governance that can become insulated from conventional reform efforts over long incubation periods.

This is not, however, solely a problem confined to the most compromised regimes. Variants of these dynamics have emerged in smaller and strategically sensitive environments, including Pacific Island states such as Palau and the Solomon Islands**,** where criminal networks linked to Chinese capital and influence have exploited regulatory gaps, political capture, and infrastructure dependencies. And, the model appears to be spreading globally. While understudied, these cases demonstrate how emerging criminal footholds can generate outsized long-run strategic effects.

---

[19] Briefing by U.S. Department of State officials to the House Select Committee on the CCP, 2026 (on file with the Committee).
[20] Jason Tower, "Exporting Fraud: China's Acquiescence to Myanmar's Military Regime Fuels 'Foreigner Butchering' Scam Epidemic," Global Initiative Against Transnational Organized Crime, October 10, 2025, https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/.
[21] Jacob Sims, *Policies and Patterns: State-Abetted Transnational Crime in Cambodia as a Global Security Threat* (Humanity Research Consultancy, 2025).

A. Harms to Americans

The harms posed by the criminal phenomenon now raging in the Indo-Pacific are in no way confined to regional instability. This ecosystem shifts risk and losses onto populations outside the region – especially in advanced economies – while shielding operators and enablers from accountability. Americans are now among the primary targets of these networks.

Financial and Psychological Harm to American Citizens

Financial losses resulting from cyber-enabled fraud linked to Indo-Pacific criminal networks have reached unprecedented levels. In September 2025, the U.S. Department of the Treasury (Treasury) assessed that Americans lose more than $10 billion annually to Southeast Asia–based networks operating scam compounds and associated laundering infrastructure.[22] As prominent American scam victim advocate and former prosecutor Erin West has warned in various public fora, "PRC-origin organized crime syndicates are stealing a generation's worth of wealth from the American public."[23]

These losses are driven disproportionately by *sha-zhu pan*, or "pig-butchering," scams – long-con fraud schemes that combine sustained social engineering with fraudulent investment platforms, often leveraging cryptocurrency and online trading interfaces. U.S. government reporting shows that these schemes are among the fastest-growing sources of victim losses, frequently resulting in catastrophic financial harm to individuals who lose retirement savings, home equity, or family assets.[24] [25]

The targeting pattern is also evolving: recent analysis has documented the rise of *sha-yang pan*, or "foreigner butchering," a Mandarin-language term used to describe fraud redirected toward non-Chinese victims, including Americans, as PRC enforcement pressure increasingly prioritizes scams against Chinese nationals.[26]

These operations are merely the visible front end of a broader cybercriminal market. Underground banking networks and crypto laundering pathways enable proceeds to be moved rapidly across borders and converted between fiat and digital assets with limited friction.[27][28] Syndicates leverage open-source APIs to optimize and scale their fraud schemes.[29] Technical reporting has also linked Cambodian scam

---

[22] U.S. Department of the Treasury, Office of Foreign Assets Control, "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams," Press Release SB0237, September 17, 2025, https://home.treasury.gov/news/press-releases/sb0237.
[23] Erin West, "Remarks on Transnational Scam Compounds and Victim Harm," presentation at Global Initiative Against Transnational Organized Crime conference on combating online scams, Bangkok, Thailand, November 2024, notes on file with Committee.
[24] FBI, *2023 Internet Crime Report* (2023).
[25] FBI, *2024 Internet Crime Report* (2024).
[26] Jason G Tower, "China's Acquiescence to Myanmar's Military Regime Fuels 'Foreigner Butchering' Scam Epidemic," Global Initiative Against Transnational Organized Crime, October 10, 2025, https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/.
[27] United Nations Office on Drugs and Crime (UNODC), *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation: A Shifting Threat Landscape* (Bangkok: UNODC ROSEAP, October 2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.
[28] Financial Crimes Enforcement Network (FinCEN), Advisory on Investment Scam Typologies and Illicit Finance (Washington, DC: U.S. Department of the Treasury, 2024).
[29] Michael Di Girolamo, *Deceptive by Design: The AI-Enabled Tools Fueling the Scam Industry* (Washington, DC: C4ADS, February 25, 2026), https://c4ads.org/issue-briefs/deceptive-by-design/

centers to malware-as-a-service infrastructure, banking trojans, credential theft, data exfiltration, remote-device surveillance, and multilingual targeting across multiple continents.[30][31]

In an unclassified briefing with the Select Committee in March 2026, officials from the U.S. Department of State described scam compound economies as a polycrime problem: cyber fraud fused with trafficking-in-persons, corruption, border management failures, and money laundering – often accelerated by crypto misuse. That interlocking structure is precisely why harms to Americans scale: the fraud is not an isolated scheme but the revenue engine of a broader illicit ecosystem that can absorb pressure and reconstitute.

Financial loss is the most visible harm to Americans, but it is not the only one. Victims of these forms of cyber-enabled scams frequently experience severe psychological and emotional trauma, including depression, anxiety, and social isolation, particularly when losses involve life savings or occur alongside manipulation of personal relationships.[32] The financial destruction and ensuing isolation have contributed to severe crisis outcomes, including numerous documented suicides.

Senior U.S. officials have increasingly framed these harms as a strategic problem rather than a series of isolated consumer fraud cases. Treasury and U.S. Department of Justice (DOJ) actions emphasize that the magnitude, persistence, and transnational character of these scams now rival other major illicit financial threats facing the United States, particularly where foreign state tolerance or protection enables their continued operation.[33] [34]

U.S. Private Sector Implications

Another important risk is private sector exposure. This exposure does not require intent or collusion. It can arise when corporate infrastructure is exploited at scale, when revenue incentives weaken enforcement posture, or when governance systems are not designed to withstand sustained, adversarial abuse by transnational criminal networks.

Financial and crypto-market infrastructure face exposure where illicit proceeds from scam operations and forced criminality are converted, laundered, or moved through U.S.-linked rails. Large jurisdictionally decentralized exchanges, such as Binance, can operate as critical chokepoints where funds derived from trafficking-enabled scam economies are legitimized or obscured, undermining sanctions regimes, victim recovery efforts, and civil litigation pathways that depend on timely cooperation with legal processes.

American technology platforms also face exposure to risk where their systems function as scalable acquisition and targeting mechanisms for transnational fraud networks. For instance, recent investigative

---

[30] Infoblox Threat Intel and Chong Lua Dao, "Scams, Slaves and (Malware-as-a) Service: Tracking a Trojan to Cambodia's Scam Centers," *Infoblox Blog*, April 10, 2026, https://www.infoblox.com/blog/threat-intelligence/scams-slaves-and-malware-as-a-service-tracking-a-trojan-to-cambodias-scam-centers/.

[31] Federal Bureau of Investigation (FBI), *Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[32] Following the Money: Tools and Techniques to Combat Fraud: Hearing before the Subcommittee on National Security, Illicit Finance, and International Financial Institutions of the U.S. House Committee on Financial Services, 119th Cong. (April 1, 2025) (written statement of Kathy Stokes, Director of Fraud Prevention Programs, AARP Fraud Watch Network), https://www.congress.gov/119/meeting/house/118056/witnesses/HHRG-119-BA10-Wstate-StokesK-20250401.pdf.

[33] U.S. Treasury, Office of Foreign Assets Control, "Treasury Sanctions Southeast Asian Networks."

[34] Criminal indictment: *United States v. Chen Zhi,* No. 1:25-cr-00312-RPK (E.D.N.Y. Oct. 8, 2025) (unsealed Oct. 14, 2025), https://www.justice.gov/usao-edny/media/1416286/dl.

reporting discusses China-based scam actors leveraging Meta's global advertising platforms to reach large volumes of potential victims and indicates that cross-border advertising flows from China-linked entities represent a significant share of detected fraudulent activity.[35] This highlights a structural vulnerability: systems optimized for reach, engagement, and revenue can be exploited by organized scam networks operating at industrial scale in permissive governance environments.

Connectivity providers may face a related but distinct exposure profile. DOJ has issued seizure warrants targeting Starlink satellite terminals allegedly used at scam compounds in Burma**,** reflecting a growing recognition that satellite connectivity can function as a force multiplier for coercive, trafficking-linked cyber-fraud operations.[36] The exposure for U.S. firms is both operational – diversion, resale, and misuse of terminals – and strategic, as continued service provision risks association with forced-labor-linked criminal enterprises.

These cases highlight a broader pattern: CCP-linked organized crime scales by exploiting private sector systems not designed for sustained, adversarial abuse**.** When governance controls are weak or incentives misaligned, U.S. firms risk becoming de facto enablers. Across numerous sectors, private infrastructure is being weaponized to facilitate victimization, sustain forced-labor models, and create consequences for U.S. interests.

For Congress, the implication is not that U.S. companies are primary wrongdoers, but that private sector governance has become a frontline national security variable**.** These networks intersect with legitimate systems not because any one firm intends harm, but because the criminal model is built to industrialize victim acquisition and move value through whatever infrastructure is available.

Penetration to the United States

These networks are no longer confined to overseas operations. Evidence indicates that transnational scam and laundering networks linked to Southeast Asia have increasingly extended their activities onto U.S. soil. These activities include the use of U.S.-based shell companies, money mules, and facilitators; the recruitment or coercion of individuals within the United States to move or launder funds; and, in some cases, the establishment of operational nodes or support infrastructure inside U.S. jurisdictions.[37] [38]

This domestic presence raises risk in two ways. First, it deepens American exposure to fraud by shortening operational chains and reducing reliance on foreign intermediaries. Second, it complicates enforcement by embedding transnational criminal activity within local communities and financial systems, blurring the line between foreign and domestic threats.

[35] Jeff Horwitz, "Meta Tolerates Rampant Ad Fraud in China to Safeguard Billions in Revenue," Reuters Investigations, December 15, 2025.
[36] Matt Burgess, "Elon Musk's Starlink Is Keeping Modern Slavery Compounds Online," WIRED, February 27, 2025, https://www.wired.com/story/starlink-scam-compounds/.
[37] 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.
[38] Criminal indictment: *United States v. Chen Zhi. (E.D.N.Y.)*

B. Harms to Regional Partners

The harms described in this report do not affect the United States alone. Countries across Southeast Asia and the Pacific are themselves bearing growing financial and governance costs, alongside severe human harm as a result of transnational scam and fraud networks embedded within the region.

Financial and Social Harms to U.S. Allies and Partners

Across the Indo-Pacific, scam-related financial losses now rival or exceed those experienced by many advanced economies when measured relative to GDP. In Thailand alone, authorities estimate that annual losses from scams exceed 115 billion Thai baht (approximately $3.5 billion at May 2026 exchange rates), [39] reflecting the scale at which transnational fraud has penetrated domestic financial systems and consumer markets.[40] Similar trends have been reported across Singapore, Korea, Japan, Indonesia, Malaysia, and the Philippines, where online fraud, investment scams, and crypto-enabled schemes have become a significant issue.

These losses carry significant secondary effects. They erode confidence in financial institutions, overwhelm law enforcement and regulatory bodies, and generate political pressure for rapid responses that are often difficult to sustain. In each of the above-mentioned countries, scam-related victimization has become a salient public issue, shaping domestic debates over corruption, foreign influence, and state capacity.

Governance Erosion and Criminal–Political Entanglement

In March 2024, then-INTERPOL Secretary General Jürgen Stock warned that organized crime groups that began as a regional threat in Southeast Asia had evolved into a global crisis driven by human trafficking and cyber scam centers, with an estimated $2 trillion to $3 trillion in illicit proceeds moving through the global financial system each year.[41]

Beyond direct financial harm, the presence of large-scale scam and gambling-adjacent operations has contributed to deeper governance challenges. In environments characterized by weak oversight or politicized enforcement, criminal enterprises have leveraged licensing regimes, investment incentives, and infrastructure development to operate behind a veneer of legality. Over time, this has enabled the formation of protection markets and corrupt alliances that insulate criminal activity from accountability.[42]

The trajectory of offshore gaming operations in the Philippines illustrates how nominally legal licensing regimes can become platforms for criminal convergence. Under the Duterte administration, Philippine Offshore Gaming Operators (POGOs) – many with links to Chinese capital and criminal networks – expanded rapidly, facilitating money laundering, labor abuses, and scam-related activity under regulatory cover.[43] While the Marcos administration has since undertaken significant crackdowns and

[39] Global Anti Scam Alliance (2025). https://gasa.org/knowledge-base/blog/thailand-faces-unprecedented-scam-crisis-with-thb-115-3-billion-lost-annually

[40] Trading Economics, "Thai Baht," spot rate USD/THB, May 5, 2026, https://tradingeconomics.com/thailand/currency.

[41] Yantoultra Ngui, "Southeast Asia Human Trafficking Now a Global Crisis, Interpol Says," *Reuters*, March 27, 2024, https://www.reuters.com/world/asia-pacific/southeast-asia-human-trafficking-now-global-crisis-interpol-says-2024-03-27/.

[42] USIP, Transnational Crime in Southeast Asia (2024).

[43] Philippine Senate Committee on Ways and Means, Committee Report No. 136: Philippine Offshore Gaming Operators (POGOs) (Senate of the Philippines, 2023).

reversals, the legacy of this period underscores how permissive governance environments can allow illicit ecosystems to scale rapidly (see Section 3.3).

Cambodia and Burma represent more extreme versions of this same pattern. In both countries, investment linked to China's Belt and Road Initiative (BRI) was unusually significant relative to the size of each economy,[44] rapidly outpacing scrutiny and creating an environment in which large infrastructure projects could acquire the political legitimacy of "development" even when embedded in high-risk or weakly regulated sectors. These permissive investment environments and expansive BRI labeling made it easier for criminally exposed actors to operate behind development narratives.

Over time, China-linked criminal enterprises linked to scams, online gambling, and illicit finance became deeply embedded in these political economies, producing concentrated hubs of illicit activity that functioned with relative autonomy from conventional regulatory controls. In Cambodia, this produced a model of criminalized stability (see Section 3.1), in which CCP-linked criminal capital became intertwined with elite protection networks and development projects that appeared legitimate. In Burma, it produced a more fragmented model of conflict-embedded criminal governance (see Section 3.2), in which scam economies became tied to militia control, border conflict, sanctions evasion, and PRC-facing financial rails.

However, the corrosive effects of these ecosystems are not confined to the most compromised states. Thailand illustrates a related but distinct form of regional exposure. Recent investigative reporting has discussed how scam-linked capital rooted in Cambodia's criminal economy moved through cross-border financial networks connected to senior Thai political and business figures. [45] In a notable case, a South African fixer is alleged to have operated between Cambodia's crime hubs,[46] CCP-linked developers,[47] and Thailand's elite economy to launder enormous illicit proceeds into Thai markets. These linkages illustrate a broader regional risk: the enormous illicit rents derived from the scam ecosystem can cultivate influence and distort governance even in more institutionalized U.S. allied and partner states.

These cases also highlight a strategic paradox. As PRC-origin criminal networks expand abroad, Beijing's efforts to pursue Chinese fugitives and suppress fraud targeting Chinese nationals can become a vehicle for deeper Chinese police influence in the same jurisdictions where those networks operate. China has increasingly framed cross-border anti-fraud and law-enforcement cooperation as part of a broader security agenda, including through the Global Security Initiative, while developing joint police mechanisms and regional coordination centers with Southeast Asian states. These arrangements may produce real tactical gains against selected criminal actors, but they can also expand Beijing's security footprint and leverage over host governments.[48]

Human Trafficking and Regional Victimization

[44] AidData. *China Global Development Dashboard*. Williamsburg, VA: William & Mary, n.d. Accessed May 12, 2026.
[45] Tom Wright, "Exposed: The $1.5B Money Laundering Network Behind Thailand's Shinawatra Dynasty," *Whale Hunting*, Project Brazen, September 11, 2025.
[46] Jacob Sims, "The Vanishing Princeling: The Dynastic Alliances That Fueled a $1.5 Billion Laundering Network and the Backlash Now Threatening Its Collapse," *Whale Hunting* (Project Brazen), October 10, 2025, https://whalehunting.projectbrazen.com/the-vanishing-princeling-the-dynastic-alliances-that-fueled-a-1-5-billion-laundering-network-and-the-backlash-now-threatening-its-collapse/.
[47] Tom Wright, "America's New Enemy: The Chinese Crypto Cartel Buying States to Fight the U.S.," *Whale Hunting*, Project Brazen, December 11, 2025.
[48] USIP, Transnational Crime in Southeast Asia (2024).

The human costs of this ecosystem extend beyond financial losses. Scam operations across the region rely heavily on forced labor, drawing victims from across Southeast Asia and beyond.

A 2025 Amnesty International investigation documents how human trafficking dynamics manifest within scam compounds. Victims reported being subjected to physical and sexual violence, debt bondage, and threats of resale to meet scam performance quotas. Many were recruited through deception, transported across borders, stripped of identity documents, and held under constant surveillance, with escape attempts met with severe and violent retaliation, sometimes resulting in death. In multiple cases, victims were forced to scam family or community members under threat of physical or sexual abuse, compounding both financial and psychological harm.[49]

Trafficking victims in scam compounds face a distinctive challenge. They are exploited as victims while being coerced to defraud a second set of victims. Criminal networks deliberately exploit this dual status to maintain control, discourage escape or cooperation with authorities, and increase victims' fear that they will be treated as offenders rather than as trafficking survivors. Enforcement responses have too often compounded this vulnerability by misidentifying coerced workers as irregular migrants or criminal suspects, limiting access to shelter, services, legal protection, and witness cooperation.

The non-punishment principle – the internationally recognized standard that trafficking victims should not be penalized for unlawful acts they were compelled to commit – is therefore not only a humanitarian safeguard but also a criminal-disruption imperative. Proper victim identification preserves access to testimony, devices, financial information, recruitment pathways, and compound-level intelligence, while prosecuting or deporting victims forecloses cooperation and strengthens impunity for compound operators.

According to U.S. government estimates, individuals from more than 80 countries have been exploited in scam compounds, with particularly high numbers originating from China and ASEAN member states including Thailand, Indonesia, Vietnam, Malaysia, and the Philippines.[50]

The 2025 Trafficking in Persons (TIP) Report also provides a framework for assessing these abuses through its treatment of state-sponsored human trafficking**.** A 2019 amendment to the Trafficking Victims Protection Act (TVPA) recognized that governments themselves can act as traffickers where the State Department identifies a government policy or pattern of conduct that enables forced labor or sexual exploitation, including through government-funded programs, government-affiliated sectors, or the systematic failure to prevent or disrupt known trafficking schemes.[51][52] The 2025 TIP Report added Cambodia to this list for the first time, specifically noting high-level state complicity in trafficking into the scam industry. China and Burma are also on this list, albeit not for forced criminality in cyber-enabled fraud.

---

[49] Amnesty International, *I Was Someone Else's Property: Forced Criminality and Human Trafficking in Scam Compounds* (London: Amnesty International, 2025).

[50] U.S. Department of State, Office to Monitor and Combat Trafficking in Persons, 2025 Trafficking in Persons Report (September 29, 2025), https://www.state.gov/reports/2025-trafficking-in-persons-report/.

[51] Trafficking Victims Protection Act of 2000, Pub. L. No. 106-386, 114 Stat. 1466 (2000), as amended, 22 U.S.C. §§ 7101 *et seq.*; *see also* Frederick Douglass Trafficking Victims Prevention and Protection Reauthorization Act of 2018, Pub. L. No. 115-425, 132 Stat. 5472 (2019).

[52] U.S. Department of State, 2025 Trafficking in Persons Report.

For the United States, these governance failures matter not only because they affect allies and partners, but because they degrade the broader regional environment impacting U.S. security, economic, and diplomatic interests. State complicity with illicit activity on this scale undermines rule of law, corrodes governance, and weakens state capacity in countries central to U.S. Indo-Pacific strategy.

C. Harms to U.S. Security Interests

The criminal ecosystem described in this report poses a direct and compounding challenge to U.S. security interests in the Indo-Pacific. While its mechanisms differ from traditional military or territorial threats, its cumulative effects – on governance, financial integrity, regional stability, and coercive leverage – are substantial and, in some cases, harder to counter. Treating this threat as peripheral or purely a law enforcement challenge undervalues both its persistence and its strategic consequences.

Erosion of the Rules-Based Order and Partner Capacity

At a regional level, CCP-linked organized crime undermines core U.S. security objectives by weakening the institutional capacity of partner states. Over time, this dynamic reduces the ability of partner governments to enforce laws, regulate markets, and cooperate effectively with the United States on shared security priorities.[53]

As multiple assessments have noted, criminal ecosystems thrive in environments characterized by selective enforcement and politicized accountability – conditions that are reinforced, rather than challenged, by certain governance preferences associated with the CCP's domestic and external engagements. The result is a regional landscape in which criminal actors can embed themselves within infrastructure, real estate, financial services, and online platforms with limited risk of sustained disruption.[54]

For the United States, this governance erosion has concrete security consequences. When criminal networks entrench themselves politically, partner states struggle to implement sanctions, regulate infrastructure, or sustain security cooperation. These weaknesses create exploitable gaps in the regional security system.

Strategic Spillover and U.S. Access Risks

These dynamics also intersect directly with U.S. military posture and strategic competition in the Indo-Pacific. The inclusion of Pacific Island states as case studies in this report (see Section 3.4) reflects not only concerns about governance and corruption, but the growing recognition that CCP-linked organized crime can undermine U.S. strategic military objectives.

In several Pacific contexts, TCOs linked to Chinese capital and business networks have established footholds through illicit finance, real estate acquisition, gambling-adjacent enterprises, and corruption. These footholds pose risks to mid-to-long term U.S. engagement and facility access by distorting and obscuring local political incentives. In such environments, the presence of organized crime is not merely a

[53] USIP, Transnational Crime in Southeast Asia (2024).
[54] USIP, Transnational Crime in Southeast Asia (2024).

background condition – it becomes a factor that complicates defense cooperation, infrastructure security, and long-term access arrangements.[55]

The sheer financial scale of these networks creates additional strategic spillover effects. Large volumes of illicit capital – generated through scams targeting Americans and regional populations – are laundered through global financial systems, including U.S.-linked institutions, cryptocurrencies, and offshore jurisdictions.[56] The Chen Zhi indictment further demonstrates that these ecosystems are not geographically bounded. The Prince Group's operations spanned more than thirty countries, maintained nodes within the United States, and leveraged U.S. infrastructure even as they operated from permissive environments abroad. Such cases collapse the distinction between foreign and domestic threats and reinforce the need for a security framework that treats organized crime as a strategic variable, not a background condition.

Implications for U.S. Strategy

Together, these dynamics warrant treating CCP-linked organized crime as a distinct national security category. The distributed nature of the threat does not make it any less dangerous. In many ways it is more difficult to counter with traditional tools. Staggering financial harm to American citizens, partner governance erosion, strategic denial risks, and security cooperation degradation cannot be meaningfully countered without addressing the criminality and corruption that shape elite behavior and state capacity. Where such realities have become entrenched, they must be treated as first-order strategic concerns.

PART II. METHODS AND APPROACHES

A. Research Design and Evidentiary Standards

This report examines two primary cases, Cambodia and Burma, and three supporting case categories: the Philippines, Pacific Island states, and emerging frontiers. These cases were selected to capture variation in regime type, institutional capacity, degree of PRC influence, and forms of organized criminal activity. Cambodia and Burma are treated as in-depth cases because evidence of criminal–state entanglement is extensive and well documented. The supporting cases are used to test how similar dynamics appear in different governance environments and at different stages of criminal metastasis.

Within each case, the analysis focuses on three factors:

1. Dominant criminal activities;
2. Pathways of CCP-linked tolerance, enablement, or exploitation; and
3. Implications for U.S. interests and potential disruption points.

Evidence Base and Evidentiary Thresholds

[55] USIP, Transnational Crime in Southeast Asia (2024).
[56] UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia* (January 2024).

The evidence base draws on a diverse set of unclassified sources, including corporate registries and beneficial ownership records; property, infrastructure, and licensing data; court documents, indictments, and enforcement actions; sanctions designations and financial advisories; satellite imagery and geospatial indicators; and targeted briefings with U.S. government agencies and private sector actors.

The investigation applied a tiered evidentiary framework throughout. Findings are categorized as direct linkages, supported by documentary evidence or official actions; strong circumstantial linkages, where multiple independent indicators point in the same direction; or suggestive but incomplete indications, which are flagged explicitly as such.

This report treats intent and outcome as analytically distinct. Centralized direction is noted where evidence warrants, but the absence of such evidence does not preclude damaging effects. This report proceeds from the premise that distributed systems can and do produce persistent harm through aligned incentives, selective enforcement, and permissive governance even when intent remains unclear, an analytic posture aligned with that observed in federal agency and other briefings.[57]

B. Typology of CCP-Linked Complicity

To enable structured comparison across cases, this report employs a typology of CCP-linked complicity in organized crime. The typology distinguishes "PRC-origin transnational criminal organizations" – Chinese-speaking criminal networks, including but not limited to PRC nationals – from "CCP-linked transnational criminal organizations," which implies some form of state tolerance, state-adjacent facilitation, or policy-relevant linkage.

The typology reflects a core analytic judgment: CCP-linked organized crime emerges from a spectrum of interactions among PRC-origin TCOs, CCP-linked actors or institutions, and permissive governance environments. Categorizing those interactions allows the report to assess severity, identify leverage points, and tailor policy responses without overstating intent.

The typology consists of three categories: passive tolerance, instrumental enablement, and strategic exploitation. These categories are not mutually exclusive. Multiple forms may coexist within a single country or criminal ecosystem, and dynamics may shift over time.

Passive Tolerance

Passive tolerance describes cases where PRC-origin TCO activity persists in part because of systematic non-enforcement or regulatory blind spots by PRC authorities, rather than active state support. In these contexts, relevant CCP or PRC institutions may be aware of illicit activity but choose not to act consistently, even where they possess the legal authority and/or operational capacity to do so.

[57] Briefers suggested it unlikely that senior PRC leadership are directing overseas scam ecosystems, while underscoring the harder question of tolerance / selective non-action within a centrally controlled system.

Indicators include prolonged non-action despite credible reporting, selective enforcement against low-level actors while higher-value networks remain untouched, permissive outbound capital and travel controls, and the absence of meaningful investigations into well-documented PRC-origin criminal enterprises operating abroad. In some cases, tolerance appears to reflect prioritization of regime stability or political relationships. In others, it appears to reflect governance preferences that place control, influence, or economic returns above transparency and rule of law.

Passive tolerance lowers operational risk and allows illicit markets to consolidate. Over time, it can become a form of de facto protection, enabling criminal enterprises to scale, relocate, and embed themselves within foreign political economies with limited fear of disruption from PRC authorities.

Instrumental Enablement

Instrumental enablement describes situations in which CCP-linked actors, state-affiliated entities, or PRC-aligned intermediaries take identifiable actions that facilitate criminal activity for economic, political, or strategic benefit. Unlike passive tolerance, enablement involves observable conduct that reduces risk or increases profitability for transnational criminal enterprises.

Such actions may include facilitation through state-linked companies, provision of access to infrastructure or capital, regulatory accommodation, protection through diplomatic or political channels, or selective crackdowns that discipline unaligned actors while preserving favored networks. In these cases, criminal activity becomes intertwined with influence-building, rent-seeking, or informal governance arrangements linked to CCP-aligned interests.

Instrumental enablement does not require centralized direction from Beijing. It often operates through decentralized incentives in authoritarian or hybrid systems, where political loyalty, revenue generation, and utility to broader influence objectives shape behavior.

Strategic Exploitation

Strategic exploitation captures cases where criminal ecosystems are leveraged, directly or indirectly, to advance broader PRC or CCP objectives, even if those ecosystems are not fully directed or controlled by the state. This may include illicit finance that generates off-budget revenue, tolerance of criminal activity that externalizes harm onto foreign populations, or sustained non-intervention where criminal outcomes align with geopolitical or strategic interests.

Evidence of strategic exploitation is often more fragmentary than evidence of tolerance or enablement, particularly in unclassified analysis. Indicators include persistent protection of high-impact criminal enterprises and noted alignment between those criminal enterprises and broader strategic goals.

Strategic exploitation does not imply that criminal networks function as formal instruments of state policy. Rather, it captures situations in which the benefits of criminal ecosystems are sufficiently aligned with CCP objectives that meaningful disruption is neither prioritized nor sustained.

This typology is applied across the country case studies that follow. Each case assesses where observed dynamics fall along the tolerance–enablement–exploitation spectrum, identifies supporting indicators, and flags evidentiary confidence levels. This approach enables structured comparison while preserving analytic restraint.

PART III. HOST COUNTRY CASE STUDIES

A. Cambodia: Stability-Embedded, State-Crime Ecosystem

Cambodia has emerged as one of the world's most consequential hubs for industrial-scale cyber-enabled fraud. Over the past decade, closed, compound-based scam operations have proliferated across the country, combining online investment deception, human trafficking for the purposes of forced criminality, and large-scale laundering through casinos, underground banking networks, the formal financial system, and cryptocurrency channels.[58] [59] The dominant "pig-butchering" model relies on prolonged social engineering conducted primarily by low-level (often exploited) workers targeting victims primarily in the United States, Europe, and East Asia.[60]

Convergent estimates from UN agencies, U.S. government reporting, and independent investigations suggest that upwards of 150,000 individuals have been trafficked into scam operations in Cambodia and that annual illicit proceeds plausibly range between $12.5 and $19 billion.[61] [62] While precise figures remain difficult to verify, there is little dispute that Cambodia's scam economy operates at industrial scale with sustained tolerance by powerful local officials. Its magnitude is sufficient not only to impose significant harm on foreign victims but also to generate elite rents within Cambodia's own political economy at a scale likely materially supportive of regime resilience.[63]

Cambodia's role cannot be understood simply as organized crime flourishing in a weak state. Rather, it reflects a politically consolidated, patronage-embedded system capable of absorbing and stabilizing large-scale illicit capital and efficiently transferring that capital to its ruling coalition.[64] [65] In this environment, enclosed scam compounds – characterized by controlled access, private security, debt bondage, and violence against trafficked workers – have operated across the country with durable local tolerance, even amid periodic publicized crackdowns.[66] [67]

At the same time, Cambodia's ecosystem did not emerge in isolation. Its rapid consolidation coincided with intensified PRC domestic campaigns against online gambling around 2010, with campaigns against telecom fraud and capital flight beginning in the mid-2010s.[68][69] As enforcement risk increased inside China, criminal networks sought offshore jurisdictions combining permissive regulation, receptive elites, and established China-facing commercial and financial channels. Cambodia's regulatory openness, dense

[58] UNODC, Transnational Organized Crime Threat Assessment: Southeast Asia.
[59] FinCEN, Advisory on Investment Scam Typologies and Illicit Finance.
[60] UNODC, Transnational Organized Crime Threat Assessment: Southeast Asia.
[61] Jacob Sims, *Policies and Patterns,* 2025, pp 5-6.
[62] USIP, Transnational Crime in Southeast Asia (2024).
[63] USIP, Transnational Crime in Southeast Asia (2024).
[64] Jacob Sims, *Policies and Patterns,* 2025, pp 11-15.
[65] Neil Loughlin, "Transnational Organised Crime Meets Embedded Corruption: Cambodia's Role in Southeast Asia's Online Scam Epidemic," *Global China Pulse* 3, no. 1 (2024): 27–34, https://doi.org/10.69131/GCP.03.01.2024.02.
[66] UNODC, Transnational Organized Crime Threat Assessment: Southeast Asia.
[67] Amnesty International, *I Was Someone Else's Property*.
[68] UNODC, Transnational Organized Crime Threat Assessment: Southeast Asia.
[69] USIP, Transnational Crime in Southeast Asia (2024).

patronage structures, and deepening economic alignment with Beijing made it a natural absorption point.[70] [71] [72]

China-facing financial rails – including underground banking networks, crypto brokers, and gambling-linked payment systems – further enabled fraud and money laundering at scale.[73] [74] Public reporting demonstrates that Chinese authorities have periodically applied diplomatic or law-enforcement pressure inside Cambodia, particularly when Chinese nationals were primary victims or when reputational costs rose.[75] Yet the durability and growth of Cambodia's scam ecosystem over multiple years indicate that offshore suppression was, until very recently, more selective rather than comprehensive.[76] Understanding this interaction – rather than attributing causality exclusively to either domestic corruption or centralized Chinese orchestration – is essential to assessing both the threat landscape and the strategic implications that follow.

3.1.2 CCP-Linked Enabling Pathways

This section examines how Chinese party-state behavior, both active and passive, helped enable the conditions in which Cambodia's scam economy emerged and persisted. The analytic focus is on how Chinese enforcement priorities, state-adjacent legitimacy systems, financial ecosystems, and geopolitical trade-offs shaped criminal risk calculations and allowed large-scale illicit activity to consolidate in a profoundly corrupted offshore environment.

Enforcement Displacement as a Structural Enabler

Beginning in the early 2010s, Chinese authorities intensified domestic campaigns against online gambling, telecom fraud, and capital flight, sharply increasing the risks of operating such enterprises inside China.[77] [78] These campaigns involved mass arrests, asset seizures, and sustained political signaling.

Crucially, however, this enforcement was primarily inward-facing. As operational risk rose inside China, criminal networks adapted by relocating offshore, seeking jurisdictions that combined permissive governance and political receptivity to Chinese capital and migrants.[79] Cambodia emerged as a preferred destination within this displacement pattern.

---

[70] Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?"
[71] UNODC, Transnational Organized Crime Threat Assessment: Southeast Asia.
[72] Arthur Eremita, "Cambodian Propaganda: Playing the Victim to Get Away With Murder," *The Diplomat*, October 31, 2023, https://thediplomat.com/2023/10/cambodian-propaganda-playing-the-victim-to-get-away-with-murder/.
[73] Financial Crimes Enforcement Network (FinCEN), *Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds,* FIN-2025-A003 (Washington, DC: U.S. Department of the Treasury, August 28, 2025), https://www.fincen.gov/system/files/2025-08/FinCEN-Advisory-CMLN-508.pdf.
[74] USIP, Transnational Crime in Southeast Asia (2024).
[75] PRC Embassy in Cambodia, press statements on joint anti-scam operations and repatriations.
[76] USIP, Transnational Crime in Southeast Asia (2024).
[77] United Nations Office on Drugs and Crime (UNODC), *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat* (Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, January 2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.
[78] Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?"
[79] USIP, Transnational Crime in Southeast Asia (2024).

The Cambodian government's 2019 online gambling ban – introduced following Chinese pressure – was a pivotal moment where this criminal displacement-absorption dynamic rapidly became a globally harmful phenomenon. Before the ban, Chinese capital, operators, and customers had helped fuel a rapid casino and online-gambling boom, especially in Sihanoukville. The ban disrupted the visible online-gambling model, but it did not dismantle the underlying ecosystem.[80] Rather, buildings, operators, labor brokers, payment channels, corrupt protection networks, and China-facing technical infrastructure remained in place and simply pivoted business models. As online gambling became more politically costly and less viable, many of these assets were repurposed into closed scam compounds reliant on coerced labor and cyber-enabled fraud.[81]

From the standpoint of the PRC involvement typology, this outcome reflects passive tolerance by externalization: domestic enforcement succeeded in reducing politically sensitive activity at home while accepting predictable offshore reconstitution as a by-product.[82]

Selective Law-Enforcement Pressure and Risk Management

Beyond displacement, PRC enforcement pressure on Cambodia-based scam networks from 2019 to 2025 is best described as selective and interest-contingent, rather than comprehensive. Public reporting and official statements document periods of China-Cambodia joint operations, extraditions, and arrests, particularly when Chinese nationals were primary victims, when capital-flight risks escalated, or when offshore criminality generated reputational costs for Beijing.[83] [84]

These interventions did not amount to sustained dismantlement. Cambodia's scam ecosystem expanded for years despite clear Chinese awareness, indicating that enforcement actions functioned primarily as risk-management tools – signaling boundaries and mitigating domestic fallout – rather than as efforts to eliminate offshore criminal markets.[85]

This selectivity matters because it suggests not enforcement incapacity or ignorance, but prioritization, in which offshore harm was tolerated until it intersected with core Chinese interests. That highly selective enforcement posture combined with a notably muted Western diplomatic-enforcement response during most of the same time period materially shaped criminal expectations and contributed to the durability and scale of Cambodia-based operations.

State-Adjacent Legitimacy Structures

PRC state-adjacent legitimacy systems – particularly those associated with the United Front and consultative political bodies – have functioned as indirect enabling mechanisms for the scam ecosystem in

[80] Ivan Franceschini, Ling Li, and Mark Bo, *Scam: Inside Southeast Asia's Cybercrime Compounds* (London: Verso, 2025).
[81] United Nations Office on Drugs and Crime (UNODC), *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia: Policy Report* (Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, September 2023), https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.
[82] USIP, Transnational Crime in Southeast Asia (2024).
[83] Tess McClure, "Age of the 'Scam State': How an Illicit, Multibillion-Dollar Industry Has Taken Root in South-East Asia," *The Guardian*, December 2, 2025, https://www.theguardian.com/technology/2025/dec/02/scam-state-multi-billion-dollar-industry-south-east-asia.
[84] PRC Embassy in Cambodia, press statements on joint anti-scam operations and repatriations.
[85] USIP, Transnational Crime in Southeast Asia (2024).

Cambodia.[86] These structures were designed to project influence and co-opt overseas elites, not to facilitate crime. They have, however, been repeatedly repurposed by criminal entrepreneurs to signal political respectability, reduce scrutiny, and secure access to host-state elites. The case of Wan Kuok-koi, a Macau triad leader sanctioned by the United States in 2020, illustrates the problem. He operated United Front–style organizations and held affiliations with the Chinese People's Political Consultative Conference, a PRC political advisory body. His case shows how China-linked legitimacy signaling can complicate enforcement without requiring direct CCP direction.[87]

Provincial and national United Front Work Department (UFWD) actors have worked with TCOs in Cambodia, giving those networks further reach and capacity to advance state political campaigns and influence.[88] In exchange, the criminal networks gain political cover and legitimacy, demonstrating the CCP's opportunistic tolerance of aligned illicit actors.[89] Such alignments do not demonstrate state sponsorship of criminal activity, but they do show how state-adjacent structures can lower operational friction for illicit actors in permissive host environments.

Elite Criminal Entrepreneurs and State Tolerance: The Chen Zhi Case

Multiple investigative and policy sources have raised – without conclusively resolving – the question of whether Chen Zhi, founder of Prince Group and the most extensively documented criminal patron in Cambodia's scam economy, functioned at times as a state-managed Chinese asset, rather than as a purely independent offshore criminal.[90] [91] [92]

There is no public documentary evidence of formal recruitment. Evidence of tasking or direction by PRC intelligence or party authorities is limited to firsthand accounts that are not fully verifiable. Nonetheless, several convergent circumstantial indicators warrant analytic attention. Chen operated at extraordinary scale for years with minimal disruption despite extensive reporting and survivor testimony; cultivated China-facing legitimacy and access to state-owned construction firms; and faced decisive PRC action only after U.S. sanctions, indictments, and asset seizures imposed significant diplomatic and reputational costs. Moreover, the first official Chinese response to the U.S.-U.K. action in October 2025 was to suggest that the U.S. seizure of the assets was improper and illegal, effectively defending Chen Zhi and attempting to cast the action as geopolitical overreach.[93]

Viewed through Chinese enforcement incentives, this trajectory is consistent with state-adjacent tolerance and management: offshore criminal actors may be tolerated so long as they remain useful, manageable, or

---

[86] Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?"
[87] U.S. Department of the Treasury, "Treasury Sanctions Corrupt Actors in Africa and Asia," press release, December 9, 2020, https://home.treasury.gov/news/press-releases/sm1206.
[88] "CCP Enlists Hongmen Crime Syndicate That Violates Nations' Sovereignty," *Indo-Pacific Defense Forum*, September 2025, accessed May 12, 2026.
[89] Jason G. Tower, "China-Linked Transnational Organized Crime in Southeast Asia: A Rising Threat to U.S. National Security," testimony before the U.S.-China Economic and Security Review Commission, Hearing on Crossroads of Competition: China in Southeast Asia and the Pacific Islands, March 20, 2025, https://www.uscc.gov/sites/default/files/2025-03/Jason_Tower_Testimony.pdf.
[90] Jacob Sims, *Policies and Patterns,* 2025, pp 16-22.
[91] Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?"
[92] USIP, Transnational Crime in Southeast Asia (2024).
[93]Vince Dioquino, "Chinese Cybersecurity Watchdog Alleges US Stole $13.2B in Bitcoin Five Years Ago," *Decrypt*, November 11, 2025, https://decrypt.co/348109/chinese-cybersecurity-watchdog-alleges-us-stole-13-2b-in-bitcoin-five-years-ago.

insufficiently costly to Chinese interests. Unclassified evidence of direct strategic exploitation of the Prince Holding Group TCO by elements of the PRC state is present but circumstantial.[94] [95]

Citizenship Laundering and Jurisdictional Shielding

An underexplored enabling pathway is Cambodia's large-scale naturalization of Chinese nationals through opaque or corrupt processes. [96] Civil-society investigations and parliamentary disclosures indicate that more than 2,500 Chinese nationals have acquired Cambodian citizenship under expedited conditions linked to investment or political patronage.[97]

For PRC-origin criminal actors, Cambodian citizenship reduces extradition risk, facilitates land and corporate ownership, and deepens integration into local protection networks.[98] From a PRC standpoint, this mechanism enables externalization of criminal risk without direct intervention: once naturalized abroad, individuals fall outside routine Chinese consular responsibility while remaining embedded in China-facing financial and social networks.[99]

Chinese Capital, Infrastructure, and Financial Rails

Beyond the documented cases of state-owned enterprise (SOE) involvement, PRC-origin capital played a decisive role in constructing the physical infrastructure later exploited by scam operations.[100] [101] The coastal Cambodian city of Sihanoukville's casino and real-estate boom produced dense clusters of high-capacity buildings well suited to confinement and call-center operations.[102]

Even where direct involvement of a Chinese SOE or policy bank in scam compounds is not established, SOE-financed infrastructure and permissive outbound capital flows created opportunity structures that criminal networks subsequently repurposed for illicit use.[103][104]

Finally, it appears that Cambodia's strategic alignment with Beijing functioned as a diplomatic buffer during key growth phases of the scam economy, reducing multilateral pressure on Phnom Penh and lowering the costs of tolerance.[105] China's posture shifted toward firmer engagement only when offshore scams imposed substantial reputational, financial, or domestic political costs.

---

[94] USIP, Transnational Crime in Southeast Asia (2024).
[95] Lintner, "Untangling Scam Kingpins' Ties to the Chinese Government."
[96] Sims, *Policies and Patterns*.
[97] Inca Digital, "Citizenship, Criminal Infrastructure, and Foreign Leverage: What Cambodia's Naturalization Data Reveals," *Inca Digital*, 2026.
[98] USIP, Transnational Crime in Southeast Asia (2024).
[99] Ibid.
[100] USIP, Transnational Crime in Southeast Asia (2024).
[101] UNODC, Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia: Policy Report (September 2023).
[102] Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?"
[103]USIP, Transnational Crime in Southeast Asia (2024).
[104] Sims, *Policies and Patterns*.
[105]USIP, Transnational Crime in Southeast Asia (2024).

3.1.3 Typology Assessment: CCP Posture Toward Cambodia-Based Organized Crime

This section assesses how the Chinese party-state has related to Cambodia-based organized crime over time, using the typology outlined in Part II: passive tolerance, instrumental enablement, and strategic exploitation. The purpose is to determine which postures are supported by observable behavior and which remain inferential given the limits of unclassified research.[106] Taken as a whole, the available evidence supports a finding that Chinese posture has been dominated by passive tolerance and instrumental enablement, while claims of strategic use remain plausible in certain situations, but not conclusively proven.

Passive Tolerance

The most strongly supported posture is passive tolerance, understood here as durable Chinese awareness of offshore criminal activity combined with the absence of sustained extraterritorial suppression sufficient to prevent consolidation and growth.[107] This tolerance should not be confused with inaction or incapacity. Chinese enforcement campaigns against online gambling, telecom fraud, and capital flight were real, often severe, and politically salient within China.

What distinguishes this posture is that enforcement remained primarily inward-facing. As risk increased domestically, criminal networks predictably relocated offshore. Cambodia-based scam ecosystems expanded and professionalized for years after Chinese authorities publicly acknowledged the problem and after policy measures – such as Cambodia's 2019 online gambling ban enacted at Beijing's urging – were in place.[108] Rather than eliminating or suppressing criminal capacity, these actions displaced it geographically.

From the standpoint of Chinese state incentives, this pattern reflects tolerance by externalization: illicit activity was pushed beyond China's borders, where its social and political costs were borne primarily by foreign victims and host-state institutions, while domestic exposure was reduced.[109] The durability of Cambodia's scam economy despite prolonged Chinese awareness strongly supports this interpretation.

Observers examining prominent Cambodia-linked cases have emphasized that prolonged non-enforcement coexisted with clear state capacity to intervene, suggesting that tolerance was conditional rather than inadvertent. Disruption occurred only once political, diplomatic, or reputational exposure escalated – underscoring the distinction between enforcement capacity and enforcement will.[110]

Instrumental Enablement

Beyond tolerance, the evidence supports a finding of instrumental enablement, defined as selective Chinese actions that shaped, stabilized, or constrained offshore criminal ecosystems without outright directing them. This posture is most visible in the interest-contingent application of law-enforcement pressure.

---

[106] USIP, Transnational Crime in Southeast Asia (2024).
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Lintner, "Untangling Scam Kingpins' Ties to the Chinese Government."

Public reporting and official statements document episodes of PRC-Cambodia joint operations, extraditions, and arrests, particularly when Chinese nationals were primary victims, when capital-flight risks escalated, or when offshore criminality generated reputational costs for Beijing.[111] These interventions demonstrate that PRC authorities possessed both awareness and leverage.

At the same time, these actions did not amount to a sustained dismantlement strategy. Cambodia's scam ecosystem expanded for years despite repeated Chinese engagement, indicating that enforcement functioned primarily as risk management rather than eradication.[112] [113]

The trajectory of Chen Zhi and the Prince Group also illustrates how instrumental enablement can operate at the elite level without formal tasking. There is no documentary evidence that Chen was recruited or directed by Chinese authorities. However, the convergence of circumstantial indicators – extraordinary operational latitude over time, cultivation of China-facing legitimacy, and decisive PRC action only after U.S. sanctions and indictments imposed significant costs – supports an assessment of state-adjacent tolerance or management, rather than mere host-state corruption.[114] [115] [116]

Strategic Exploitation

By contrast, the available evidence does not establish strategic exploitation, defined again as deliberate Chinese use of Cambodia-based organized crime to advance affirmative state objectives such as coercive foreign policy, centralized control over illicit markets, or direct revenue generation. While the aforementioned individual reports raise the possibility that Prince Holding Group and Chen Zhi functioned as developed assets,[117] there is no public documentation of CCP directives to offshore criminal activity and no conclusive evidence of high-level Chinese political orchestration across Cambodian networks.

3.1.4 Case-Distinct Impacts to U.S. Interests

The broader harms associated with convergent CCP-linked organized crime in Cambodia – including direct financial losses to American victims and strain on U.S. financial enforcement – are addressed in Part I.B. This section offers additional Cambodia-specific impacts to U.S. strategy and interests.

Strategic Competition and Leverage Asymmetry

PRC-backed development and use of Ream Naval Base has rightly drawn U.S. attention in Cambodia.[118] A sustained Chinese military presence in the Gulf of Thailand would affect regional force posture and maritime balance. As a result, U.S. policy has focused heavily on transparency, conditional engagement,

---

[111] Embassy of the People's Republic of China in the Kingdom of Cambodia, press statements on joint anti-scam operations and repatriations, 2024.
[112] Jacob Sims, *Policies and Patterns*, 2025, pp 19-22.
[113] USIP, Transnational Crime in Southeast Asia (2024).
[114] Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?" RFA, February 5, 2024.
[115] DOJ USAO-EDNY, "Chairman of Prince Group Indicted," October 14, 2025.
[116] Grant Peck, "Alleged Scam Kingpin Chen Zhi Arrested in Cambodia," Associated Press, January 7, 2026, https://apnews.com/article/cambodia-scam-chen-zhi-prince-group-china-b32da55af90841d6b2b95cc6334f3fa7.
[117] Davies, "Cambodia's Prince Group: A Business Empire Built on Crime?" RFA, February 5, 2024.
[118] United States Department of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China (Washington, DC: U.S. Department of Defense, 2024).

and incentives tied to Cambodian security cooperation. But a Cambodia strategy organized too narrowly around Ream risks mistaking a visible symptom of Chinese influence for its deeper source.

The scam economy complicates this strategy insofar as it has drawn to the fore how profoundly Cambodia's political economy is intertwined with opaque, CCP-linked financial networks that generate large-scale rents through casinos, real estate, underground banking systems, and cyber-enabled fraud.[119][120] These flows operate through patronage structures that provide durable resources to political and security elites. In that environment, the traditional tools of U.S. influence – incremental engagement, aid conditioning, capacity support, and public legitimation – are structurally outmatched by the scale and flexibility of rents available through China-linked economic and illicit channels. This creates a glaring leverage asymmetry that leaves U.S. planners underprepared for denial-of-access risks in a potential conflict.

The implication is not that cyber fraud is strategically more consequential than a naval facility. It is that military access and denial risks cannot be assessed apart from the political economy that shapes Cambodian elite preferences. In other words, a narrowly Ream-centric strategy may miss the deeper alignment mechanisms that make Cambodia receptive to Chinese security access in the first place. U.S. policy therefore needs to treat criminalized political economy in Cambodia as a first-order strategic variable, not a secondary governance concern.

Sanctions Credibility and Enforcement Leverage

The 2024 Treasury sanctions against Cambodian senator and business tycoon Ly Yong Phat and several of his businesses under the Global Magnitsky Act marked an important milestone in U.S. strategy. For the first time, Washington targeted a Cambodian political and economic elite with direct ties to the ruling class for alleged involvement in trafficking-linked scam operations.[121] Yet, at the time of this report's publication, the Cambodian government has not opened a credible investigation or taken meaningful enforcement action despite mounting evidence. The case therefore illustrates both the importance and the limits of elite-targeted sanctions in a political economy where protection networks remain intact.

U.S. indictments, sanctions designations, and asset seizures – including large-scale cryptocurrency forfeitures – have imposed real costs on scam-invested Cambodian ruling elites and their PRC criminal counterparts. But sanctions do not achieve their full strategic effect through legal designation alone. Their deterrent and accountability value also depends on sustained public diplomacy and local signaling. In the Ly Yong Phat case, a Khmer-language rollout or visible U.S. Embassy amplification strategy would have increased the measure's utility as a public accountability tool.

For U.S. sanctions policy, this dynamic presents a credibility challenge. The issue is not whether sanctions can raise costs – they can – but whether episodic pressure can alter structural incentives inside a

[119] USIP, Transnational Crime in Southeast Asia (2024).
[120] United Nations Office on Drugs and Crime (UNODC), Transnational Organized Crime Threat Assessment: Southeast Asia (Vienna: UNODC, 2023–2024).
[121] United States 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," September 12, 2024, https://home.treasury.gov/news/press-releases/jy2576.

politically consolidated protection economy. Transnational accountability efforts have generally been met by adaptation and reconstitution efforts from complicit regime elites.[122] [123]

The trajectory from here likely depends on political will: whether the United States and its partners are prepared to target actors sufficiently high within Cambodia's elite patronage structures to signal that protection itself carries consequences, even at the risk of bilateral friction. It also, notably, depends on evidence access. As Cambodian civic space narrows and journalists, survivor-support organizations, and civil society investigators face mounting pressure, sanctioning governments may have fewer reliable channels for surfacing abuses, mapping protection networks, and sustaining follow-on accountability.

Civic Space, Survivor Protection, and Accountability Capacity

It is not a coincidence that Cambodia's scam economy has expanded in an environment where independent accountability actors face growing pressure. Journalists, frontline service providers, labor advocates, and civil society investigators have played an outsized role in documenting scam compounds and complicit elites, identifying and supporting victims, and sustaining international attention.[124] Yet these actors operate amid narrowing civic space, political intimidation, and legal and financial risk.[125] [126]

Funding cuts to key civil society actors compound this problem by weakening precisely the networks most capable of surfacing abuses that state authorities are unwilling or unable to confront.[127] For U.S. policy, this is not a peripheral democracy-promotion issue. In Cambodia, independent civil society functions as core accountability infrastructure. When that infrastructure is weakened by funding cuts, criminal actors evade scrutiny and U.S. sanctions or law-enforcement actions become more dependent on government narratives or episodic external intelligence rather than sustained local visibility.[128]

B. Burma: Conflict-Embedded Criminal Governance

Unlike Cambodia – where PRC-origin TCO capital integrated into centralized elite patronage networks – Burma's scam ecosystem is territorially anchored in militia-governed border enclaves shaped by decades of fragmented sovereignty and armed autonomy.[129] Yet, Burma has emerged not as a simple failed-state vacuum for crime, but as a governance environment in which armed actors control territory, administer quasi-enclave jurisdictions, and monetize protection, all meaningfully enabled by Chinese diplomatic and enforcement choices.[130] [131] Within this landscape, industrial-scale "pig-butchering" investment fraud has

[122] Jack A. Davies, follow-on investigative reporting on Cambodia's scam economy and enforcement dynamics, 2024–2026.
[123] Jacob Sims, "Crackdown, Chaos, or Cover-Up in Cambodia?," *The Diplomat*, February 11, 2026.
[124] Danielle Keeton-Olsen, "Scam Stories Hinge on On-the-Ground Journalism," *Global China Pulse* 3, no. 1 (2024), https://globalchinapulse.net/scam-stories-hinge-on-on-the-ground-journalism/.
[125] Human Rights Watch, "Cambodia: Investigative Journalist Arrested on Baseless Charge," October 3, 2024, https://www.hrw.org/news/2024/10/03/cambodia-investigative-journalist-arrested-baseless-charge.
[126] U.S. Department of State, *2025 Trafficking in Persons Report: Cambodia*, September 2025, https://www.state.gov/reports/2025-trafficking-in-persons-report/cambodia/.
[127] Amy Gunia, "Cuts to US Foreign Aid Are Hurting Efforts to Tackle Human Trafficking at Scam Compounds," *CNN*, March 10, 2025, https://edition.cnn.com/2025/03/10/world/us-funding-human-trafficking-scam-compounds-spc-hnk/index.html.
[128] Mech Dara, "A Month on Phnom Penh Streets After a Year Trapped in Scams," *Mekong Independent*, February 28, 2026, https://mekongindependent.com/2026/02/a-month-on-phnom-penh-streets-after-a-year-trapped-in-scams.
[129] Michael Di Girolamo, "Hot Lines: Tracing Movements to and from Myanmar's Scam Centers," C4ADS, March 27, 2025.
[130] USIP, Transnational Crime in Southeast Asia (2024).
[131] International Crisis Group, *Transnational Crime and Geopolitical Contestation along the Mekong*, Report No. 332 (Brussels: International Crisis Group, August 18, 2023), https://www.crisisgroup.org/asia/south-east-asia/myanmar/332-transnational-crime-and-geopolitical-contestation-mekong.

consolidated alongside longstanding borderland illicit economies, including casino gambling, narcotics trafficking, and informal cross-border trade.

Prior to the 2021 coup, semi-autonomous regions such as Kokang, Wa, Mong La, and parts of Karen State already operated under ceasefire arrangements that limited central oversight in exchange for political stability.[132] These arrangements produced durable regulatory gray zones in which casino enclaves and quasi–Special Economic Zone developments blurred licit and illicit activity.[133] Scam compounds later expanded within precisely these characteristics: territorial insulation, armed protection, and connectivity to Chinese-language commercial and financial networks.[134]

The February 2021 military coup accelerated this trajectory. The collapse of national regulatory enforcement, fragmentation of territorial control, and proliferation of armed actors seeking revenue streams transformed preexisting gray zones into active protection markets. Scam compounds also became strategic terrain within Burma's conflict economy. Armed actors have not only profited from them, but also used their presence, removal, or alleged protection to justify territorial offensives, appeal to external pressure, and delegitimize rival forces. Burma did not originate the contemporary scam model; rather, its post-coup conflict economy supplied sanctuary, coercive labor control, and political insulation sufficient for rapid industrial-scale expansion.

This relationship is central to the policy implications of the Burma case. The State Administrative Council (SAC) and its aligned militias should not be treated as neutral enforcement partners standing outside the scam economy. In many of the most important hubs, actors aligned with or tolerated by the SAC have supplied the territorial control, armed protection, and political insulation that allowed scam operations to scale. The regime has therefore survived not only despite the criminal economy, but in part through the revenue streams, coercive partnerships, and protection markets that the criminal economy sustains.[135]

This expansion unfolded within a broader regional environment shaped by intensified PRC domestic crackdowns on online gambling, telecom fraud, and capital flight beginning in the mid-2010s.[136] As enforcement risk rose inside China and parallel tightening occurred in other Mekong jurisdictions,[137] Chinese-language gambling and fraud networks relocated toward permissive border territories offering insulation from centralized state control. Burma's militia-administered enclaves absorbed that displacement, integrating PRC-linked managerial personnel, crypto-based platforms, and underground financial channels intersecting with Chinese markets.[138]

Geographically, scam compounds have clustered along porous international borders. The Thai–Burma frontier around Myawaddy became the epicenter of post-coup growth, with sites including KK Park,

---

[132] International Crisis Group, *Transnational Crime and Geopolitical Contestation along the Mekong*.
[133] USIP, Transnational Crime in Southeast Asia (2024).
[134] United Nations Office on Drugs and Crime, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia: Policy Report*, September 2023; Priscilla A. Clapp and Jason Tower, "Myanmar's Criminal Zones: A Growing Threat to Global Security," United States Institute of Peace, November 9, 2022.
[135] Michael Di Girolamo, "Hot Lines: Tracing Movements to and from Myanmar's Scam Centers," C4ADS, March 27, 2025.
[136] Jason G. Tower, "China-Linked Transnational Organized Crime in Southeast Asia: A Rising Threat to U.S. National Security," testimony before the U.S.-China Economic and Security Review Commission, March 20, 2025; UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia*, January 2024.
[137] Priscilla A. Clapp and Jason Tower, "Myanmar's Criminal Zones: A Growing Threat to Global Security," USIP, November 9, 2022; Jason Tower and Priscilla A. Clapp, "China Forces Myanmar Scam Syndicates to Move to Thai Border," USIP, April 22, 2024.
[138] USIP, Transnational Crime in Southeast Asia (2024).

Huanya, and Dongjiang reportedly housing tens of thousands of workers at peak capacity.[139] Farther north, Kokang hosted substantial operations until late 2023, when armed conflict and Chinese pressure disrupted Laukkai's hub.[140] Disruption in one node has repeatedly triggered geographic reconfiguration rather than systemic collapse.[141] In an interview for this report, transnational crime expert Jason Tower described a layered geography in Karen State: a visible outer belt of river-border compounds subject to intermittent scrutiny, alongside a more insulated inland belt relocated away from direct observation – an adaptive structure that preserves core capacity while presenting periodic infrastructure "crackdowns" as progress.[142]

Financial measurement remains difficult in a conflict environment characterized by opacity and fragmentation. Estimates draw on victim reporting, blockchain tracing, investigative journalism, and extrapolation from compound size.[143] Nevertheless, multiple independent data streams converge on the conclusion that Burma hosts one of the largest concentrations of industrial-scale cyber-fraud operations globally.[144]

Crucially, the ecosystem's durability reflects more than the country's instability. It is the product of interaction: PRC-linked criminal capital and managerial expertise; enforcement displacement from China-centric and PRC-provoked regional crackdowns; Chinese-facing underground banking and crypto rails; and Burma's militia-based protection markets supplying territory and coercive control.[145] The result is a structured transnational corrupted and criminal ecosystem in which borderland governance, cross-border finance, and digital fraud operations reign supreme.

3.2.2 CCP-Linked Enabling Pathways

Burma's scam ecosystem is sustained through layered enablement across SAC-aligned militia protection and enclave governance, supported by China-linked capital and laundering systems and selective cross-border enforcement dynamics. At the operational level, protection is supplied primarily by Burma armed actors. However, the ecosystem's rapid expansion cannot be separated from Chinese domestic crackdowns on gambling, telecom fraud, and capital flight, which increased risk inside China and redirected networks toward permissive border jurisdictions.[146] Burma's border militias absorbed that displacement.

For instance, in Karen State, the Karen Border Guard Force (BGF) – a paramilitary force aligned with Burma's military – effectively franchised territory to PRC-linked TCOs. Its commander, Saw Chit Thu, brokered land concessions and security services for scam investors and was later designated by the U.S.

---

[139] UNODC, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia*, 2023; Jason Tower and Priscilla A. Clapp, "China Forces Myanmar Scam Syndicates to Move to Thai Border," USIP, April 22, 2024.
[140] International Crisis Group, *Transnational Crime and Geopolitical Contestation along the Mekong*.
[141] UNODC, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia*, 2023; Jason Tower and Priscilla A. Clapp, "China Forces Myanmar Scam Syndicates to Move to Thai Border," USIP, April 22, 2024.
[142] Interview with Jason Tower, transnational crime expert, March 15, 2026.
[143] FBI, *Internet Crime Report*, 2024.
[144] UNODC, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia*, 2023; USIP, *Transnational Crime in Southeast Asia*, 2024.
[145] USIP, *Transnational Crime in Southeast Asia*, 2024; UNODC, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia*, 2023; Jason Tower and Priscilla A. Clapp, "China Forces Myanmar Scam Syndicates to Move to Thai Border," USIP, April 22, 2024.
[146] Jason G. Tower, testimony before USCC, March 20, 2025; UNODC, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia*, January 2024.

Treasury for his role in facilitating cyber scam operations.[147] Under his leadership, the BGF leased enclaves such as KK Park and Shwe Kokko and deployed armed personnel to secure their perimeters.[148] Survivor reporting indicates militia members enforced discipline within compounds and prevented escape attempts.[149]

The role of Burma's military is central to this arrangement. China has generally exerted pressure on scam compounds in Karen State indirectly, by pressing the Burma military to act against abuses by its aligned BGF rather than by intervening directly against BGF leaders.[150] This indirect pressure has exposed the junta's own dependency on militia partners. When pressure on Saw Chit Thu and the BGF has intensified, the group has repeatedly threatened to distance itself from formal BGF status, operate under the Karen National Army label, or align more closely with anti-junta forces.[151] These threats create a deterrent effect: the Burma military has incentives to reduce pressure in order to prevent the defection of an armed actor important to its borderland control.[152]

China appears to have tolerated this dynamic. Unlike in Kokang, where PRC authorities issued arrest warrants and pursued coercive action against military-aligned BGF leaders after Chinese interests were directly threatened, Beijing has not applied comparable direct pressure against Saw Chit Thu. This contrast suggests that Chinese enforcement posture is shaped not only by anti-scam objectives, but also by conflict-management priorities. In Karen State, Beijing has accepted a mediated and limited enforcement model in which pressure flows through the Burma military but stops short of actions that could destabilize an important junta-aligned militia.

The resulting arrangement reflects instrumental enablement: PRC-linked criminal capital, Burma's military-aligned militia system, and selective Chinese enforcement converging within a permissive geopolitical gray zone. It is a triangular structure in which China-linked criminal capital is protected by militia-based territorial governance, mediated by the Burma military's dependence on armed proxies, and tolerated by Beijing when full enforcement would threaten broader conflict-management interests.[153]

Regulatory Permissiveness and Enclave Governance

Scam compounds in post-coup Burma operate under the cover of development projects, casino concessions, or Special Economic Zone (SEZ) frameworks – where regulatory and legal scrutiny are often suspended – while functioning as fortified enclave jurisdictions in practice.[154] [155]

Shwe Kokko's Yatai New City illustrates this model. Initially framed as a multibillion-dollar development under the prior civilian government, it evolved into a militia-administered enclave with minimal

[147] U.S. Department of the Treasury, "Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scam Operations," press release, May 5, 2025.
[148] USIP, Transnational Crime in Southeast Asia (2024).
[149] UNODC, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia*, 2023
[150] Interview with Jason Tower, transnational crime expert, March 15, 2026.
[151] Interview with Jason Tower, transnational crime expert, March 15, 2026.
[152] Ibid.
[153] Interview with Jason Tower, transnational crime expert, March 15, 2026.
[154]Priscilla A. Clapp and Jason Tower, "Myanmar's Criminal Zones: A Growing Threat to Global Security," United States Institute of Peace, November 2022.
[155] United States Institute of Peace, *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security* (Washington, DC: USIP, 2024).

oversight.[156] Notably, early public messaging by Yatai and some Chinese interlocutors associated the project with the Belt and Road Initiative, lending it symbolic legitimacy before subsequent investigations and reputational fallout distanced it from formal BRI branding.[157] The episode demonstrates how BRI-adjacent signaling – even absent formal designation – can create political insulation and complicate external scrutiny.

A 2020 investigation identified investment irregularities and suspended expansion; after the 2021 coup, oversight effectively collapsed, enabling rapid consolidation.[158]

Long-standing autonomy arrangements in Kokang, Wa, and Mong La – originating in the 1989 ceasefires – restricted central enforcement in exchange for political stability and created durable regulatory voids later repurposed for cyber-fraud operations.[159] Kokang, however, followed a more specific post-2009 trajectory. After the Burmese military defeated the Myanmar National Democratic Alliance Army (MNDAA) and brought the area under tighter military-aligned control, former MNDAA-linked elites and defectors – including the Bai, Liu, and Wei clan networks – became Border Guard Force (BGF)-aligned power brokers. According to an interview with transnational crime expert Jason Tower, Kokang's later emergence as one of Burma's largest scam hubs reflected a clear political bargain: support for the Burmese military and its Union Solidarity and Development Party (USDP)-aligned political order in exchange for latitude to build and protect large-scale scam, gambling, and illicit-finance empires.[160] Preexisting casino infrastructure and cross-border trade networks were then repurposed for cyber-fraud operations after 2021, allowing Kokang's scam economy to scale rapidly once post-coup enforcement collapsed.[161] These BGF-linked criminal economies also recycled funds back into the military-aligned political economy, making them revenue-generating pillars of regime-aligned control rather than merely tolerated criminal enterprises.[162]

Compounds also exploit cross-border jurisdictional fragmentation. Electricity, telecommunications, and supply chains often originate in Thailand or China while enforcement responsibility remains territorially constrained.[163] Junta crackdowns have frequently appeared selective; reporting indicates operators were sometimes forewarned or relocated prior to raids.[164][165] However, since 2025, scam compounds on the Thailand-Burma border have increasingly used generators and internet from Burma and Mytel – a military-owned mobile network operator – highlighting the Burma military's direct involvement in powering and supplying critical resources for scam activities.[166]

---

[156] Tower and Clapp, *Myanmar's Casino Cities*, pp 8-10.
[157] Ibid
[158] USIP, Transnational Crime in Southeast Asia (2024).
[159] International Crisis Group, *Transnational Crime and Geopolitical Contestation along the Mekong*, 2023; Priscilla A. Clapp and Jason Tower, "Myanmar's Junta Is Losing Control of Its Border with China," USIP, November 8, 2023.
[160] Interview with Jason Tower, transnational crime expert, March 15, 2026.
[161] Priscilla A. Clapp and Jason Tower, "Myanmar's Junta Is Losing Control of Its Border with China," USIP, November 8, 2023
[162] Interview with Jason Tower, transnational crime expert, March 15, 2026.
[163] Panarat Thepgumpanat and Panu Wongcha-um, "Thailand to Cut Power to Myanmar Border Areas Linked to Scam Centres," *Reuters*, February 4, 2025.
[164] Panarat Thepgumpanat and Panu Wongcha-um, "Thailand to Cut Power to Myanmar Border Areas Linked to Scam Centres," *Reuters*, February 4, 2025.
[165] Hannah Beech, "At This Office Park, Scamming the World Was the Business," *The New York Times*, January 13, 2026, https://www.nytimes.com/2026/01/13/world/asia/myanmar-scam-center.html.
[166] Briefing by Jason Tower to House Committee, March 15, 2026.

A recent episode involving the Karen National Union/Karen National Liberation Army (KNU/KNLA) underscores both the potential and the constraints of non-state disruption in Burma. In late 2025, the KNLA seized control of the Shunda scam compound in Min Let Pan, documented evidence and devices, and attempted to process detainees. The absence of coordinated cross-border intake, investigative support, victim-screening capacity, and stabilization assistance left the operation difficult to sustain, and many suspects ultimately dispersed.

The Shunda episode also carried territorial significance. According to an interview with transnational crime expert Jason Tower, Min Let Pan had been associated with DKBA influence, and DKBA-linked actors were widely understood to be closer to the military-aligned ecosystem than the KNU. The presence of a scam compound in this border area created an opening for the KNU/KNLA to leverage international anti-scam pressure, challenge a rival armed actor's control, and bring a strategically important crossing under its own authority.

It also demonstrated the enforcement value of evidence recovered by non-regime actors. In April 2026, DOJ announced charges against two Chinese nationals alleged to have managed fraud operations at Shunda, after FBI agents working with Thai authorities reviewed thousands of devices and hard drives recovered from the compound and interviewed former workers.[167] DOJ stated that the investigation identified a hierarchical organization of Chinese operators and supported charges against a high-level manager/enforcer and a team leader who supervised workers targeting American victims.[168] The lesson is not that armed organizations can substitute for a functioning state. It is that credible anti-scam strategy in Burma will require channels that can support responsible non-regime actors where they control relevant territory, particularly for evidence preservation, victim protection, safe-transfer protocols, and cross-border investigative coordination.

Real Estate and Infrastructure Enablement

The physical architecture of Burma's scam hubs was largely constructed through PRC-linked private and diaspora capital working in partnership with militia actors. She Zhijiang (Dylan She), founder of Yatai International Holdings, played a central role in developing Shwe Kokko. His joint venture with Saw Chit Thu's Chit Linn Myaing Company formed Yatai International Holdings Ltd., structured 70/30 between Chinese investor and militia-linked partner. The U.S. Treasury Department also identified Trans Asia International – a Thailand-registered firm with Chinese investors – as a developer of scam parks in Karen State operating alongside militia partners. Across sites, enabling infrastructure appears to have been driven predominantly by private capital tied to gambling and gray finance networks rather than by Chinese SOEs or policy-bank financing, distinguishing Burma's infrastructure pattern from more formal state-linked development models visible elsewhere in the region.

Financial Rails

Scam proceeds are laundered through transnational networks deeply intertwined with Chinese-language shadow banking systems. Victim funds are typically extracted through cryptocurrency or layered via

[167] U.S. Department of Justice, "Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans," press release, April 23, 2026, https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting.
[168] U.S. Department of Justice, "Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans," April 23, 2026.

shell accounts before integration.[169] In 2025, the U.S. Treasury Department's Bureau of Financial Crimes Enforcement Network (FinCEN) designated Huione Group as a primary money laundering concern, illustrating the regional infrastructure linking Southeast Asian scam networks to Chinese underground banking channels.[170]

Newer compounds have reduced reliance on satellite connectivity and reportedly shifted toward Burma telecom services, while expanding use of local Burma payment systems alongside couriers and informal value transfer.[171] If sustained, this would modestly change disruption points by increasing reliance on junta-controlled or junta-tolerated domestic infrastructure even as the broader laundering architecture remains Sino-centric.

Chinese underground banks and over-the-counter (OTC) crypto brokers have played documented roles in converting digital assets into RMB or other currencies.[172] Burma's Financial Action Task Force (FATF) blacklisting in 2022 further incentivized reliance on crypto, cash smuggling, and informal value transfer systems rather than formal banking channels.[173] This financial architecture is PRC-centric in structure but not demonstrably state-directed, reflecting private criminal finance embedded within broader Chinese-language shadow banking ecosystems.

Cross-Border Facilitation & PRC Law-Enforcement Posture

China's posture toward Burma-based scam networks shifted significantly after 2022. Early expansion phases were characterized by domestic enforcement and public warnings focused on internal stability; overseas hubs were secondary.[174] As Chinese nationals increasingly became victims, Beijing escalated its response.[175]

In an unclassified briefing, U.S. State Department officials stressed that PRC action tends to accelerate when reputational costs rise or when harms to PRC nationals become salient – producing episodic, highly public enforcement bursts that may or may not translate into sustained constraint.[176] That pattern is consistent with this report's interpretation of posture shifts in Burma as recalibration under political constraint rather than a durable dismantlement strategy.

In 2023, PRC authorities intensified cross-border coordination. The United Wa State Army repatriated thousands of Chinese nationals from Wa territory which fundamentally destabilized the existing political order in the north of the country and led to a significant EAO-led counter-insurgency movement known

[169] FBI, *Internet Crime Report*, 2024.
[170]FinCEN, *Advisory on Investment Scam Typologies and Illicit Finance*, 2024; FinCEN, "FinCEN Finds Cambodia-Based Huione Group to Be of Primary Money Laundering Concern," May 1, 2025.
[171] Briefing by Jason Tower to House Committee, March 15, 2026.
[172] Ibid.
[173] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, Regional Office for Southeast Asia and the Pacific, April 2025.
[174] Priscilla A. Clapp and Jason Tower, "Myanmar's Criminal Zones," USIP, November 9, 2022; Jason G. Tower, testimony before USCC, March 20, 2025.
[175] Priscilla A. Clapp and Jason Tower, "Myanmar's Junta Is Losing Control of Its Border with China," USIP, November 8, 2023; Jason G. Tower, "Exporting Fraud," GI-TOC, October 10, 2025.
[176] Unclassified briefing by U.S. Department of State officials to the House Select Committee on the Chinese Communist Party, March 2026, notes on file with the Committee.

as Operation 1027.[177] Following Operation 1027 and the collapse of Kokang militia control, Chinese authorities pursued prosecutions against Kokang BGF leaders for large-scale fraud.[178] Subsequent court sentences underscored Beijing's willingness to impose severe penalties when domestic political costs rise.[179]

Operation 1027 also illustrates the agency of conflict actors in weaponizing anti-scam pressure. The MNDAA and allied forces were not merely passive beneficiaries of Chinese frustration with Kokang-based scam operations; they leveraged Beijing's pressure on military-aligned Border Guard Force actors to reclaim territory and reframe their offensive as both a political-military campaign and an anti-crime corrective. In this sense, PRC enforcement pressure became an input into Burma's battlefield dynamics, shaping the timing, legitimacy, and consequences of territorial realignment.

Following Operation 1027 – after militia forces aligned with the SAC suffered territorial losses – China's posture shifted toward more visible diplomatic and material support for the junta. This recalibration suggests that anti-scam enforcement and conflict outcome management became intertwined, reinforcing interpretations of instrumental risk management rather than purely technocratic crime control.[180]

3.2.3 Typology Assessment

To characterize CCP linkage to Burma's scam economy, this section again evaluates evidence across a spectrum: tolerance, instrumental enablement, and strategic exploitation. The objective is to locate the most defensible interpretation of PRC posture within an ecosystem in which Burma's armed actors supply territorial sanctuary and coercive governance.[181]

Across available evidence, Burma's case clusters most strongly in the middle of this spectrum. Early tolerance and permissive externalization are evident during relocation into border enclaves; instrumental enablement is visible through PRC-linked criminal capital, infrastructure investment, financial intermediation, and selective enforcement; claims of deliberate strategic use by the CCP remain unproven, though certain enforcement shifts intersect with broader conflict management dynamics.[182]

---

[177] Xinhua (China's official state news agency), "Over 1,200 Telecom Scam Suspects from Northern Myanmar Handed Over to China," *Xinhua News Agency*, September 8, 2023, https://english.news.cn/20230908/9c2969e65abd41698bd963c6805db7e7/c.html.
[178] Priscilla A. Clapp and Jason Tower, "Myanmar's Junta Is Losing Control of Its Border with China," USIP, November 8, 2023; *The Irrawaddy*, "China Arrest Warrant Names Kokang BGF Founder as Top Suspect in Myanmar Cyber Scam," December 11, 2023
[179] Xinhua, "Chinese Courts Conclude Trials of Two Criminal Gangs from Northern Myanmar, 16 Sentenced to Death," February 26, 2026; *Global Times*, "China Executes 4 Leading Members of Northern Myanmar-Based Bai Criminal Gang," February 2, 2026.
[180] Jason G. Tower, "Exporting Fraud: China's Acquiescence to Myanmar's Military Regime Fuels 'Foreigner Butchering' Scam Epidemic," GI-TOC, October 10, 2025.
[181] UNODC, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia*, 2023; USIP, *Transnational Crime in Southeast Asia*, 2024; Jason Tower and Priscilla A. Clapp, "China Forces Myanmar Scam Syndicates to Move to Thai Border," USIP, April 22, 2024.
[182] International Crisis Group, *Transnational Crime and Geopolitical Contestation along the Mekong*.

Passive Tolerance

In Burma's scam context, tolerance is most evident in the formative period (approximately 2017–2020), when online gambling and fraud networks consolidated in semi-autonomous border enclaves operating in longstanding regulatory gray zones.[183]

One indicator is the extent to which PRC-adjacent local political economies treated militia-linked enterprises as legitimate cross-border actors. Analysts document patterns in which Chinese provincial authorities maintained commercial engagement with Kokang elites despite the region's entrenched reputation for casino-linked criminality.[184] This does not demonstrate central CCP sponsorship, but reflects permissive local governance and weak early enforcement incentives before scams generated acute domestic political costs.

A second indicator is delayed coercive action against prominent Chinese nationals operating in Burma's border developments. She Zhijiang operated publicly for years before heightened PRC action culminated in an Interpol Red Notice in 2022.[185] Regional reporting on other high-profile scam entrepreneurs linked to Burma's border economy similarly highlights the gap between visibility and enforcement – reinforcing the analytic distinction between enforcement capacity and enforcement will in PRC posture toward offshore hubs.[186] In 2023, the PRC demanded the Burma military junta shut down the scam operations on the China-Burma border; after the military failed to comply over the course of months, the situation reached a breaking point when BGF guards opened fire on compound workers attempting to escape, resulting in the deaths of several Chinese nationals. In an aggressive response, the PRC conducted a cross-border sting operation, facilitated kidnappings, and issued arrest warrants targeting Kokang elites.[187][188] This clear example of PRC capability to act decisively and assertively when its own interests are threatened reveals the breadth of tolerance it otherwise displays.

Also notable, during the expansion phase, Shwe Kokko was at times publicly associated with Belt and Road Initiative rhetoric, lending symbolic legitimacy before later distancing.[189] While such posturing is not necessarily a sign of formal sponsorship, it does create perceived insulation. BRI-associated symbolism can deter host-state scrutiny, complicate third-party responses, and provide criminal entrepreneurs a low-cost way to borrow political legitimacy in gray-zone environments.

---

[183] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, Regional Office for Southeast Asia and the Pacific, April 2025.
[184] Jason Tower and Priscilla A. Clapp, *Myanmar's Casino Cities*, USIP, July 2020; Jason G. Tower, testimony before USCC, March 20, 2025.
[185] Jason Tower and Priscilla A. Clapp, *Myanmar's Casino Cities*, USIP, July 2020; Al Jazeera, "Under Siege in Myanmar's Cyber-Scam Capital," July 29, 2024. Use a separate direct source for the Interpol Red Notice if keeping that specific Red Notice claim.
[186] Lintner, "Untangling Scam Kingpins' Ties to the Chinese Government."
[187] Jason Tower, "Myanmar's Junta is Losing Control of Its Border with China," USIP, November 8, 2023, https://www.usip.org/publications/2023/11/myanmars-junta-losing-control-its-border-china.
[188] "China Arrest Warrant Names Kokang BGF Founder as Top Suspect in Myanmar Cyber Scam," *The Irrawaddy*, December 11, 2023, https://www.irrawaddy.com/news/burma/china-arrest-warrant-names-kokang-bgf-founder-as-top-suspect-in-myanmar-cyber-scam.html.
[189] Jason Tower and Priscilla A. Clapp, *Myanmar's Casino Cities*, USIP Special Report No. 471, July 2020.

Tolerance during this period appears driven less by strategic intent than by jurisdictional complexity, uneven central–local incentives, and the fact that early harms were largely externalized. That posture became politically unsustainable as Chinese nationals became prominent victims.[190]

Instrumental Enablement

Evidence of instrumental enablement is substantial across multiple layers.

At the PRC criminal network layer, Burma functioned as a sanctuary jurisdiction enabling continued targeting of foreign victims while complicating PRC domestic enforcement.[191] Supervisors, technical managers, and gambling-linked syndicates migrated into border enclaves and adapted existing models into cyber-fraud ecosystems enforced through coercion and trafficking.[192]

At the private and diaspora capital layer, infrastructure development materially enabled scam consolidation. Joint ventures pairing Chinese capital with militia-linked land and protection partners – such as Yatai's 70/30 structure in Shwe Kokko – demonstrate formalized investment mechanisms underpinning enclave construction.[193]

The 2024 Al Jazeera documentary in which She Zhijiang claimed to have been affiliated with Chinese intelligence – while unverified and plausibly self-serving – illustrates the reputational ambiguity surrounding some actors operating at the intersection of criminal enterprise and state-adjacent systems.[194] The claim itself does not establish state direction, but its resonance underscores blurred perceptions in regional political economies.

At the state-adjacent level, Chinese law enforcement's selective overseas interventions reflect instrumental logic: pressure intensifies when Chinese nationals are primary victims or when border instability threatens core interests.[195] Criminal operators adapt accordingly, shifting victim pools or relocating geographically.

Taken together, these indicators support classification within instrumental enablement: profit-seeking criminal and private actors embedded in CCP-linked networks operating within an enforcement environment shaped by uneven risk tolerance and episodic intervention.[196]

Strategic Exploitation

No credible public evidence demonstrates that Beijing intentionally cultivated scam enclaves as a strategic tool. Authoritative sources consistently attribute the industry's growth to criminal

[190] Jason G. Tower, "Exporting Fraud," GI-TOC, October 10, 2025; Xinhua, "Over 1,200 Telecom Scam Suspects from Northern Myanmar Handed Over to China," September 8, 2023.
[191] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, Regional Office for Southeast Asia and the Pacific, April 2025.
[192] USIP, Transnational Crime in Southeast Asia (2024).
[193] Tower and Clapp, *Myanmar's Casino Cities*.
[194] Al Jazeera, "Under Siege in Myanmar's Cyber-Scam Capital."
[195] UNODC, *Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia: Policy Report* (September 2023).
[196] USIP, Transnational Crime in Southeast Asia (2024).t

entrepreneurship interacting with Burma's conflict economy rather than to CCP-directed planning.[197][198] However, enforcement dynamics complicate a simplistic dismissal of strategic implications. Following Operation 1027 and significant territorial losses for military junta-aligned militias, analysts note that China's posture shifted toward more visible diplomatic and material support for the junta. This recalibration suggests that anti-scam enforcement and conflict outcome management became intertwined, even if not originally conceived as a strategic exploitation strategy.

In other words, while the scam ecosystem does not appear to have been created or sustained as an instrument of CCP statecraft, enforcement responses have clearly intersected with broader CCP geopolitical objectives. Beijing's leverage over Wa authorities, selective pressure on militias, and subsequent support adjustments reflect pragmatic risk management rather than a coherent plan to weaponize criminal economies.

China's detention of Bao Junfeng, the United Wa State Army (UWSA) deputy commander and heir apparent reportedly linked to Wa-area scam compounds, has provided Beijing with direct leverage over Wa leadership since September 2023. Although Bao has not been publicly charged by Chinese authorities, Beijing has used his continued detention to press the UWSA to comply with Chinese conflict-management priorities, including reducing support for the Shan State Progress Party (SSPP), and MNDAA in late 2025 as China pushed the MNDAA and TNLA toward ceasefire arrangements. If accurate, this suggests that scam-compound enforcement has not merely reflected anti-fraud policy or reputational risk control. It has also been instrumentalized as a tool of Chinese Party-state leverage within Burma's conflict environment. The most defensible interpretation, therefore, is not centralized strategic design of the scam economy, but adaptive strategic exploitation: Beijing tolerates, suppresses, or selectively leverages criminal exposure depending on how enforcement interacts with broader border-stability and conflict-management objectives.[199]

Importantly, the scam industry has inflicted significant reputational, social, and financial harm on Chinese interests, including large-scale victimization of Chinese citizens. These costs are difficult to reconcile with a theory of deliberate cultivation. The more defensible interpretation is that Chinese authorities tolerated and unevenly policed offshore criminal activity until domestic political costs rose, at which point selective enforcement escalated – sometimes with secondary geopolitical effects.[200]

3.2.4 Case-Distinct Impacts to U.S. Interests

While broader harms emanating from CCP-linked criminal convergence are addressed in Part I, Burma's scam ecosystem affects U.S. interests in two structurally distinct ways compared with other regional hubs.

Conflict Finance and Sanctions Integrity

Burma's scam hubs operate within militia-controlled territories that also host narcotics production, arms trafficking, and other illicit enterprises. Revenues from cyber-enabled fraud are integrated into militia and regime survival strategies, reinforcing armed actors already subject to U.S. sanctions. Unlike more

[197] USIP, Transnational Crime in Southeast Asia (2024).
[198] International Crisis Group, *Transnational Crime and Geopolitical Contestation along the Mekong*.
[199] Interview with Jason Tower, transnational crime expert, March 15, 2026.
[200] Xinhua, "Over 1,200 Telecom Scam Suspects from Northern Myanmar Handed Over to China."

centralized environments, the Burma case involves a decentralized conflict economy in which scam proceeds function as self-financing streams for armed groups resistant to external pressure.

This convergence has two implications for U.S. national security. First, cyber-fraud revenue reduces the coercive leverage of sanctions by providing alternative funding channels to sanctioned entities and their affiliates. Second, the laundering infrastructure supporting these operations – often routed through PRC-centric shadow banking systems, crypto exchanges, and cross-border underground finance – creates pathways that can be exploited by other sanctioned or hostile actors, including those engaged in sanctions evasion or proliferation-sensitive transactions. Even absent evidence of PRC state direction, the intersection of Burma's conflict economy with PRC-facing financial rails creates enforcement vulnerabilities for U.S. authorities that extend beyond fraud itself.

Risks of Normalizing the SAC as a Counter-Scam Partner

The Burma case also carries a direct warning for U.S. and allied policy: counter-scam engagement should not become a pathway for normalizing the SAC as a legitimate or reliable state partner. The regime and its aligned militias are not external to the scam economy. They have supplied, tolerated, or benefited from the territorial protection, infrastructure access, and coercive governance arrangements that allow scam hubs to operate. Treating the SAC as an indispensable part of the solution risks strengthening the very actors whose survival strategies are intertwined with the problem.

This does not mean that all tactical deconfliction or humanitarian coordination is impossible. It does mean that engagement premised on SAC-led enforcement is likely to produce selective disruption, managed relocation, or political theater rather than systemic dismantlement. In a conflict economy where scam proceeds help sustain sanctioned actors, cooperation with the SAC can also weaken sanctions credibility, marginalize non-regime accountability actors, and reinforce the junta's claim to international legitimacy.

Border Instability and Alliance Management

Burma's scam enclaves are concentrated along sensitive border regions adjacent to Thailand and China. Enforcement cycles – whether initiated by PRC pressure, militia fragmentation, or armed conflict – have repeatedly triggered territorial shifts and cross-border instability. Operation 1027 illustrates how anti-scam disruption can intersect with broader conflict dynamics, reshaping control among ethnic armed organizations and the SAC.

The same dynamic can also be exploited by the junta. The SAC and aligned actors have increasingly invoked alleged scam-compound activity in contested northern Shan and borderland territories in ways that can blur the line between anti-crime enforcement and coercive conflict operations against rival armed groups such as the SSPP or TNLA.[201] Some of these claims may identify real criminal activity, but they also function politically: the presence or allegation of scam centers can be used to recast military offensives as anti-crime enforcement rather than as efforts to regain territory. This creates a difficult

[201] Interview with Jason Tower, transnational crime expert, March 15, 2026; SHAN, "Junta's Offensive Against SSPP in Kyaukme Township," December 1, 2025; Mizzima, "TNLA-Controlled Towns in Myanmar's Shan State Face Continuous Airstrikes, 5 Dead in 3 Days,"

policy environment in which anti-scam pressure can be instrumentalized by multiple conflict actors, including the SAC itself.

Instability along the Thai–Burma border directly affects a U.S. treaty ally. In addition, PRC law-enforcement leverage over armed groups such as the United Wa State Army likely demonstrates Beijing's capacity to influence cross-border security outcomes without formal state-to-state intervention. Even when framed as crime control, such leverage intersects with broader strategic competition by shaping local power balances and constraining the policy space available to other external actors, including the United States.

C. The Philippines: Expansion, Inflection, and Reversal

Under the CCP-aligned administration of President Rodrigo Duterte, the Philippines became one of the fastest-scaling hubs of offshore gambling-linked criminal convergence in Southeast Asia. What began as a state-licensed offshore gaming sector expanded rapidly between 2016 and 2019, attracting tens of thousands of foreign workers and hundreds of operators. Over time, segments of this ecosystem evolved into multi-layered criminal platforms combining online fraud, trafficking, forced criminality, and money laundering exposure. The Philippines did not ultimately come to replicate the entrenched territorial criminal zones of Cambodia or Burma. But it certainly approached a meaningful inflection point of truly industrial scale. The subsequent disruption under President Ferdinand Marcos Jr. demonstrates both the seriousness of the risk and the potential reversibility of such systems.

3.3.1 Strategic Alignment and Sectoral Expansion (2016–2022)

The rapid growth of POGOs followed Duterte's 2016 strategic pivot toward Beijing. Duterte publicly recalibrated Philippine foreign policy, deprioritizing defending the Philippines' interests in the South China Sea while expanding economic engagement with the PRC. Within this broader realignment, offshore gambling was licensed and promoted as a revenue-generating industry.

POGOs were regulated by the Philippine Amusement and Gaming Corporation (PAGCOR), a government entity that both licensed and derived revenue from the sector. This dual role embedded a structural conflict of interest: the same institution charged with oversight had strong fiscal incentives to expand licensing. By 2019, estimates suggest as many as 300 operators – including licensed and gray-market entities – were active, employing tens of thousands of workers, predominantly Chinese nationals.[202] [203] PAGCOR's revenues from POGOs surged during this period, and the sector became visible across Metro Manila, Clark/Angeles, Cavite, and other regions.

Beijing publicly objected to offshore gambling targeting mainland Chinese clients and periodically called for tighter controls.[204] Yet during the peak expansion period, there is no evidence that the PRC exercised meaningful leverage to constrain the ecosystem. This asymmetry is significant. Duterte's government deepened bilateral ties with Beijing across infrastructure, trade, and diplomatic domains, and PRC-origin

[202] Neil Jerome Morales, "Philippines to Start Winding Down Operations of Offshore Gaming Hubs," Reuters, July 23, 2024.
[203] Philippine Senate Committee on Ways and Means, Committee Report No. 136: Philippine Offshore Gaming Operators (POGOs) (Senate of the Philippines, 2023).
[204] Embassy of the People's Republic of China in the Republic of the Philippines, "Remarks by Chinese Embassy Spokesperson on Issues of Chinese Citizens Concerning Philippine Casinos and POGOs," August 8, 2019.

networks operated during a period of expanding strategic alignment. Whether due to prioritization of broader geopolitical objectives, limits of extraterritorial enforcement, or tacit tolerance so long as activities remained offshore, the result from Beijing was effective permissiveness.

Simultaneously, immigration and visa pathways facilitated rapid labor inflows. Visa-on-arrival policies and weak interagency integration allowed large numbers of foreign nationals to enter under minimal scrutiny. Later investigations exposed corruption within immigration channels, including bribery schemes that enabled entry of POGO-linked workers and high-risk individuals.[205] These structural vulnerabilities – combined with concentrated real estate development catering to POGOs – created enclave-like concentrations in certain jurisdictions.

Industrial-scale criminal convergence does not require initial illegality. In the Philippine case, it emerged from a legally sanctioned sector operating under conditions of regulatory mismanagement, immigration vulnerability, and geopolitical shielding.

Convergent Criminality Under Semi-Protected Infrastructure (2019–2023)

By 2019, law enforcement reporting began documenting a surge in criminal activity associated with POGOs. The most visible early indicator was kidnapping. Philippine police recorded a significant rise in kidnapping-for-ransom cases linked to gambling and POGO networks, many involving Chinese nationals targeting other Chinese nationals.[206] [207] These cases reflected the presence of organized criminal groups operating within and around POGO clusters.

Over time, segments of the POGO ecosystem shifted beyond gambling. Raids in 2022–2024 uncovered large-scale online scam operations embedded within POGO-linked facilities. In several high-profile cases, law enforcement rescued hundreds of foreign nationals allegedly coerced into conducting investment and cryptocurrency fraud targeting victims globally.[208] [209] International reporting placed the Philippines among regional destinations where "tens of thousands" were trafficked into online scam operations, though on a smaller scale than Cambodia or Burma.[210]

The convergence mechanism was straightforward. Gambling operations provided:

- physical office space and secure compounds;
- multilingual labor pools;
- device and SIM infrastructure;
- financial flows linked to offshore betting; and
- local protection buffers.

[205] Teresita Ang-See, "Chinese Migrants and the Philippines: The Need to Plug Legal Loopholes," Fulcrum, December 24, 2024.
[206] Dona Magsino, "Kidnapping Cases Up in 2019 Due to POGOs, Casinos – Police," GMA News Online, December 11, 2019.
[207] Cristina Chi, "PNP Recorded Four Times More POGO-Related Crimes in 2022 Than 2019," PhilStar.com, January 31, 2023.
[208]Christopher Lloyd Caliwan, "Report on Bamban POGO Raid," Philippine News Agency, March 2024.
[209] Joann Manabat, "Authorities Raid POGO Compound in Tarlac over Alleged Human Trafficking," *Rappler*, March 13, 2024, https://www.rappler.com/nation/luzon/raid-pogo-compound-tarlac-march-13-2024/.
[210] Office of the United Nations High Commissioner for Human Rights (OHCHR), "Hundreds of Thousands Trafficked to Work as Online Scammers in South-East Asia," August 29, 2023.

These elements proved readily repurposable for high-margin illicit activities. While not every POGO functioned as a scam compound, the architecture proved highly adaptable, and multiple documented cases resembled enclave-style infrastructure associated with forced criminality.

Money laundering exposure further compounded risk. As convergence deepened, the gambling framework increasingly served as a cover environment for broader transnational illicit finance.

3.3.2 Protection, Patronage, and Strategic Permissiveness

The scaling and persistence of criminal convergence were enabled by overlapping layers of insulation. First, regulatory conflict. PAGCOR's revenue dependency reduced institutional incentives for aggressive enforcement. While enforcement actions occurred, they were often reactive rather than systemic.

Second, immigration corruption. The so-called "pastillas" bribery scheme exposed large-scale corruption within immigration processing, facilitating the entry of POGO-linked workers.[211] Identity and documentation vulnerabilities later surfaced in multiple investigations.

Third, local political facilitation. In some jurisdictions, law enforcement failures or alleged collusion enabled POGO-linked operations to persist until national authorities intervened.[212]

Fourth, geopolitical alignment. While Beijing publicly criticized offshore gambling, the Duterte administration's broader strategic alignment with China coincided with maximal sector expansion. PRC-origin criminal networks operated in this environment. This is not evidence of top-down CCP direction. It is evidence that geopolitical alignment did not translate into meaningful constraint during peak scaling.

The convergence that emerged was therefore not solely the product of isolated corruption or criminal opportunism. It reflected an ecosystem in which licensing, migration flows, patronage networks, and geopolitical incentives aligned to reduce friction for PRC-origin criminal actors.

The Alice Guo Case: Political Penetration and Influence Risk

The Alice Guo case represents the clearest documented instance in Southeast Asia of a local elected official directly linked to POGO-associated enclave infrastructure tied to Beijing-linked networks.

Guo, elected mayor of Bamban, Tarlac, was later found to have significant irregularities in her identity and documentation. Fingerprint and civil registry reviews indicated inconsistencies in her claimed Filipino background, and her citizenship status was ultimately voided.[213] [214] Subsequent investigations linked her to ownership and corporate structures associated with a large POGO-linked compound raided by authorities in 2024. The raid uncovered alleged trafficking and scam operations involving hundreds of foreign nationals.[215] [216]

---

[211] Ang-See, "Chinese Migrants and the Philippines," *Fulcrum*, December 24, 2024.
[212] Cabalza, Dexter. 2023. "Pasay Police Chief, 26 Other Cops Sacked Over Raided POGO."
[213] Elizabeth Marcelo, "Ombudsman Orders Dismissal of Guo," The Philippine Star, August 14, 2024.
[214] Felix K. Iglesias, "The Problem With POGOs," The Diplomat, July 2024.
[215] Caliwan, "Report on Bamban POGO Raid,"
[216] Viviana Chan, "POGO Mayor Alice Guo Handed Life Sentence for Human Trafficking," Asia Gaming Brief, November 2025.

The Alice Guo case unfolded amid intense public controversy in the Philippines, with lawmakers, media commentators, and security officials openly raising the possibility that her irregular identity documentation and ties to POGO-linked infrastructure could reflect more than conventional corruption. Several senators publicly questioned whether her ascent to municipal office represented a form of foreign malign influence or infiltration.[217] This debate was fueled by the convergence of unusual factors: falsified or inconsistent civil registry records, opaque corporate networks tied to a major POGO-linked compound later raided for trafficking and scam operations, and proximity to strategically sensitive areas in Central Luzon.

Although no public evidence conclusively established espionage or state-directed tasking, the fact that credible political actors considered that possibility – and did so in a formal oversight context – underscores the gravity of the vulnerabilities exposed. The controversy itself is analytically significant: revealing how the intersection of migration loopholes, enclave-style criminal infrastructure, and electoral access can generate plausible pathways for foreign malign influence, even in the absence of a confirmed intelligence finding.

For U.S. and Philippine national security planners alike, that plausibility is not trivial.

3.3.3 Inflection Point and Disruption Under Marcos Jr. (2022–Present)

The Marcos administration recalibrated Philippine foreign policy, deepening defense cooperation with the United States and elevating national security framing. Simultaneously, domestic backlash against POGO-linked criminality intensified and gathered political steam. Legislative scrutiny increased, and enforcement tempo accelerated. Multi-agency raids dismantled major POGO-linked compounds. Public condemnation from the executive branch reframed the sector as a security liability. By mid-2024, Marcos announced the termination of POGO operations, with licenses cancelled and the sector effectively shuttered by year's end.[218]

Empirically, the licensed footprint contracted sharply. Large enclave-style sites were dismantled. Scam operations did not disappear entirely, but they shifted from semi-protected infrastructure toward fragmented, illicit remnants requiring continuous enforcement.

In this sense, the Philippine case demonstrates reversibility. The scam industry expanded when governance was permissive and political conditions favored Beijing-linked networks. It began to recede when political priorities shifted and enforcement became more coordinated.

The Philippines case illustrates how a licensed offshore sector can become enabling architecture for transnational criminal convergence when regulatory conflict, immigration vulnerability, corruption, and geopolitical alignment reduce friction for foreign-linked networks. It also demonstrates how rapidly such systems can scale under conditions of permissiveness.

---

[217] Office of Senator Risa Hontiveros, "Statement of Senator Risa Hontiveros on the Conviction of Alice Guo," Senate of the Philippines, November 20, 2025.

[218] Hsiao Tien Tan, Paris Buti, and Nigel Sharman, "The Fall of POGOs: Behind the Facade of Legality in the Philippines Offshore Gaming Space," *Hogan Lovells*, August 19, 2024.

At its apex, the POGO ecosystem exhibited industrial characteristics: large labor pools, enclave-style facilities, trafficking-linked scam operations, and laundering exposure. The Alice Guo episode revealed the plausibility of local political penetration linked to such infrastructure.

Unlike Cambodia or Burma, however, the Philippine state ultimately reasserted control. Political transition altered incentive structures, enforcement intensified, and the licensed architecture was dismantled.

The strategic lesson is not that convergence requires state sponsorship. It is that convergence flourishes where state incentives, regulatory design, and geopolitical alignment create permissive space. And that space, once created, can become materially significant for both domestic governance and allied national security interests.

D. Pacific Island States: Illicit Capital and Strategic Exposure

Pacific Island states are not currently characterized by Cambodia-style, state-criminal collaboration or Burma's conflict-derived criminalized governance. Nor have they reached the industrial-scale inflection point of the Philippines' POGO-based criminal infrastructure. Their strategic relevance to the United States, however, means that even emerging footholds of CCP-linked illicit finance, opaque investment, and governance compromise can generate outsized security consequences.

Accordingly, this case assesses Pacific Island states, centered on Palau, Solomon Islands, Vanuatu, and the Republic of the Marshall Islands (RMI), as a strategic vulnerability cluster where (i) small-state governance and anti-money laundering (AML) capacity constraints, (ii) opaque capital inflows and shell structures, and (iii) CCP-linked business networks and influence activity can intersect to create leverage asymmetries and oversight blind spots. The emphasis is thus on structural exposure and risk pathways.

Political alignment also matters. Small states can be decisive in multilateral forums and regional institutions. Accordingly, foreign influence operations may target elites and information environments precisely because political capture is "cheap" relative to conventional coercion in micro-polities. Where influence succeeds, downstream effects can include shifts in diplomatic recognition, security cooperation, investment screening decisions, and tolerance for external security presence.[219] In this context, illicit or opaque capital is strategically relevant not because it necessarily builds a globally consequential "crime hub," but because it can buy access, shape policymaking, and degrade the transparency necessary for U.S. and partner situational awareness.

3.4.1 Financial Opacity and Governance Fragility

Across the focus states, open sources repeatedly converge on a common exposure profile: thin AML/CTF capacity, limited financial intelligence capabilities, weak beneficial ownership transparency, and high reliance on external capital inflows.[220] The risk is not simply that illicit funds enter; it is that institutions

[219] Freedom House, *Freedom in the World 2024: Solomon Islands* (Washington, DC: Freedom House, 2024).
[220] Carreon, Yvette Tan, and Emmanuel Stoakes, "Foreign Workers, Local Sponsors: Inside Palau's Hotel Scam Centers," *OCCRP (Organized Crime and Corruption Reporting Project)*, December 22, 2025, https://www.occrp.org/en/investigation/foreign-workers-local-sponsors-inside-palaus-hotel-scam-centers.

may be unable to detect, investigate, or prosecute – creating permissive conditions for regulatory arbitrage and elite-level brokerage.

Palau illustrates how these governance scale constraints can become serious operational vulnerabilities. Investigative reporting based on official Palau government reporting and leaked materials discusses scam operations in repurposed hotel facilities, involving foreign workers and online fraud linked to crypto-based laundering.[221] While these operations do not appear to have grown to an industrial scale at the staggering level of Cambodia or Burma, they pose the prospect of a similar trend, with significant long-run risks.

Vanuatu's citizenship-by-investment (CBI) program, often framed as a development finance tool, has been treated by external authorities as a financial integrity vulnerability due to due-diligence and security screening concerns. The EU's revocation of Vanuatu's visa-free access explicitly cites security and money-laundering risks linked to "golden passports," representing an unusually direct external policy action grounded in perceived integrity deficits.[222] Domestic reporting also reflects official acknowledgement of risk via inquiries into whether "undesirable" individuals, including wanted criminals, obtained passports through the scheme.[223] This is evidence of a structural channel through which high-risk individuals – including those linked to transnational finance crimes – can obtain new identities and travel privileges. In an unclassified briefing, State Department officials specifically highlighted Vanuatu's "golden passport" scheme as a known vulnerability that can enable criminal mobility, jurisdictional shielding, and malign foreign influence.[224] This emphasis strengthens the case for treating CBI weakness as a strategic exposure pathway rather than merely a financial-integrity footnote.

RMI's governance fragility appears in a distinct but comparable form: susceptibility to bribery schemes aimed at reshaping sovereign authorities and legal regimes. The Rongelap "special administrative region" proposal, supported through bribes to lawmakers by foreign entrepreneurs later prosecuted in U.S. court, demonstrates how a small legislature can be targeted with comparatively modest funds to advance a far-reaching legal carve-out.[225] Here, the vulnerability is less about financial sector scale than about elite capture mechanics in a microstate.

Solomon Islands' exposure often presents as a political economy vulnerability at the intersection of foreign financing, patronage, and governance—in a context where transparency is limited and where constituency-level funds and external capital can be leveraged to consolidate political coalitions.[226] Reporting and assessments note corruption allegations and patronage dynamics, including claims of payments and inducements tied to pro-Beijing political outcomes.[227][228] This is an alarming signal of how

[221] Carreon, Tan, and Stoakes, "Foreign Workers, Local Sponsors."
[222] Council of the European Union, "Vanuatu: Council Ends Visa Exemption," press release, December 12, 2024; Philip Blenkinsop, "EU Revokes Vanuatu's Visa-Free Travel for Its 'Golden Passport' Scheme," *Reuters*, December 12, 2024.
[223] ABC Pacific (Australian Broadcasting Corporation), "Vanuatu to Launch Inquiry into Golden Passport Scheme," Pacific Beat, June 13, 2023.
[224] Unclassified briefing by U.S. Department of State officials to the House Select Committee on the Chinese Communist Party, March 2026, notes on file with the Committee.
[225] Singh, Shailendra Bahadur. "The Marshall Islands Mini-State Plot and the Price of Sovereignty in the Pacific." *The Strategist*, Australian Strategic Policy Institute, September 13, 2022.
[226] Freedom House, *Freedom in the World 2024.Solomon Islands.*
[227] Radio Free Asia / PACNEWS. 2023. "Suidani Ousted After Turning Down Chinese Bribes, Former Premier Says." May 3, 2023.
[228]Freedom House, *Freedom in the World 2024.Solomon Islands.*

governance fragility can turn otherwise conventional foreign capital into a high-leverage geopolitical instrument in small systems where oversight and enforcement are thin.

3.4.2 CCP-Linked Capital and Political Economy Dynamics

Evidence across the cluster points to China-originating business networks operating along a spectrum: from state-owned or state-connected firms pursuing infrastructure and telecom projects, to business intermediaries, to transnational criminal facilitators. The central analytic task is to avoid collapsing these categories while still recognizing that opacity and network overlap can create strategic risk even absent proof of state direction.

Palau provides the clearest documented intersection between PRC-originating illicit networks and local political economy. U.S. Treasury sanctions designations identify a Cambodia-based TCO (Prince Group) and associated facilitators tied to commercial interests in Palau, including an island lease and resort project structured through corporate entities.[229] Reporting describes documentary corporate linkages and identity/alias dynamics associated with individuals connected to the Prince network and Palau projects.[230] Separately, investigations describe Palau-based scam facilities running online fraud and gambling/investment scams, with proceeds routed via cryptocurrency and enabled by local sponsorship and regulatory gaps.[231] Taken together, these sources support the assessment that Palau has been operationally exposed to PRC-origin TCO business networks using ostensibly legitimate investment structures.[232]

Solomon Islands is best understood through influence-economy dynamics rather than confirmed illicit finance prosecutions in open sources. The attempted lease of Tulagi Island by a Chinese state-linked company, voided by the central government as unlawful, demonstrates how opaque or irregular dealmaking can target strategic real estate with potential dual-use implications.[233] Broader assessments emphasize Chinese influence methods in the Pacific, including economic leverage, diplomatic engagement scale, and security/police cooperation footprints.[234] While open-source reporting does not show entrenched illicit finance networks comparable to other cases, the country's governance constraints and capital dependence create conditions that could be exploited.

Vanuatu presents a different category of risk centered on its CBI program. External authorities have judged vulnerabilities in the program to be serious enough to warrant action. The European Union revoked Vanuatu's visa-free travel privileges, citing concerns related to security and money laundering. Domestically, the government has launched inquiries into the integrity of the program.[235]

Media reporting has also highlighted concerns that intermediaries may exploit due-diligence weaknesses to sell passports to higher-risk applicants, including individuals seeking to evade law enforcement or

---

[229] 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.
[230] OCCRP. 2025a. Adamović Davies, Jack, et al. "How Sweeping Sanctions Missed a Business Partner in the Pacific." November 26, 2025.
[231] Carreon, Tan, and Stoakes, "Foreign Workers, Local Sponsors."
[232] Carreon, Tan, and Stoakes, "Foreign Workers, Local Sponsors."
[233] Jonathan Barrett, "Solomon Govt Says Chinese Lease of Island 'Unlawful,'" *Reuters*, October 25, 2019, https://www.reuters.com/article/us-solomonislands-china/solomon-govt-says-chinese-lease-of-island-unlawful-idUSKBN1X40G0/.
[234] Freedom House, *Freedom in the World 2024.Solomon Islands.*
[235] ABC Pacific, "Vanuatu to Launch Inquiry."

financial scrutiny.[236] While this does not establish CCP direction, it demonstrates that weak screening in identity programs can create opportunities for sanctions evasion and identity laundering, complicating allied monitoring and enforcement.

RMI illustrates how foreign entrepreneurial networks can intersect with corruption vulnerabilities in a strategically significant Compact of Free Association (COFA) state. The Rongelap proposal involved bribery of lawmakers to establish a semi-autonomous administrative zone with unusual governance authorities. U.S. prosecutions and subsequent visa restrictions on implicated officials confirm that corruption was central to the effort.[237] This case does not establish CCP state control. It does, however, demonstrate that foreign capital can be used to pursue legally transformative outcomes in a small, strategically important state through targeted corruption.

3.4.3 Strategic Risk Pathways

The evidentiary picture does not support claims that the Pacific Islands cluster presently hosts mature convergent criminal activity at scale. For each country, open sources emphasize vulnerability conditions rather than confirmed large-scale criminal entrenchment. The key risk factors include: (i) limited AML and investigative capacity, (ii) high dependence on external capital and patronage financing, (iii) limited beneficial ownership transparency, and (iv) pathways for identity/mobility arbitrage (golden passports; digital residency concepts) that can be exploited by illicit actors.[238] The more significant current risk is enabling conditions, which can allow small-scale criminal experiments to scale rapidly if external pressure displaces operators from more contested jurisdictions.

Even without mature criminal ecosystems, the interaction of opaque capital and governance fragility creates several strategic risk pathways:

1. Elite capture and regulatory arbitrage: Micro-polities can be influenced through concentrated bribery aimed at legislative or permitting outcomes.[239]
2. Strategic infrastructure leverage: Opaque deals targeting ports/airfields/islands or telecom infrastructure can create U.S. and allied access constraints, information exposure, or crisis-time denial risks even if projects are nominally commercial.[240]
3. Oversight blind spots: Financial opacity (shells, layered ownership structures) and identity programs (CBI) can impede sanctions enforcement, attribution, and monitoring of high-risk actors transiting through strategically important jurisdictions.[241][242]

[236] Christopher Cottrell, "Vanuatu's Golden Visa Scheme Draws Asian Investors – and Security Scrutiny," *South China Morning Post*, May 9, 2025, https://www.scmp.com/week-asia/people/article/3309755/new-office-vanuatu-golden-visas-phuket-puts-citizenship-sale-risks-spotlight.
[237] ASPI (Australian Strategic Policy Institute). 2022. Singh, Shailendra. "Marshall Islands
[238] ABC Pacific, "Vanuatu to Launch Inquiry."
[239] OCCRP. 2023. "US Bans Entry to Marshall Islands Politicians Over China-Linked Bribery Scheme." December 12, 2023.
[240] Reuters. 2019. Barrett, Jonathan. "Solomon Govt Says Chinese Lease of Island 'Unlawful.'" October 25, 2019.
[241] OCCRP. 2025a. Adamović Davies, Jack, et al. "How Sweeping Sanctions Missed a Business Partner in the Pacific." November 26, 2025.
[242] ABC Pacific, "Vanuatu to Launch Inquiry."

4. Security footprint ratchet: Where crime, unrest, or "asset protection" narratives intensify, Chinese security cooperation offers can expand—potentially increasing Chinese security presence and influence in internal security institutions.[243]

These pathways do not require high-level CCP tasking to matter; they operate through structural incentives, asymmetries in capacity, and the strategic geography of the region.

3.4.4 Typology Placement

On the tolerance / enablement / exploitation framework, the open-source record best supports classifying the Pacific cluster as primarily vulnerable to passive tolerance dynamics, with periodic signs of instrumental enablement and strategic exploitation mechanisms (e.g., bribery attempts; opaque strategic leasing efforts).[244][245]

At a high level, the Pacific cluster is best characterized as strategically vital terrain with heightened exposure to opaque capital and governance fragility, where documented cases (notably Palau and RMI) show that PRC-linked criminal or influence-adjacent networks can operate through investment structures and corruption mechanisms even absent mature criminal ecosystems.[246][247]

E. Emerging Frontiers: Diffusion, Replication, and Early Warning Indicators

Mature criminal ecosystems rarely dissolve under concentrated enforcement pressure. Instead, they fragment, hedge, and relocate into jurisdictions where regulatory discretion, political insulation, and commercial density reduce operational risk.[248] Beginning in 2022, intensified crackdowns in Southeast Asia, combined with sanctions designations, FATF scrutiny, and diplomatic pressure, raised the costs of operating large, visible scam compounds in Cambodia and Burma. As pressure mounted, elements of the ecosystem adapted outward rather than collapsing.[249]

Emerging evidence suggests that elements of the Southeast Asian model are now diffusing into parts of East and West Africa, Latin America, South Asia, and the Middle East – typically at smaller scale and in more hybridized forms.[250] Some cases involve compound-style coercive facilities; others reflect distributed criminal operators embedded within legitimate-seeming commercial environments. In several instances, reporting intensified following enforcement surges in Southeast Asia between 2023 and 2025, though causal linkage remains inferential rather than conclusively demonstrated.

The analytic question is therefore not whether Southeast Asia's industrial-scale model has been fully replicated elsewhere. It has not. It is where documented operational presence exists, where early-stage

---

[243] Freedom House, *Freedom in the World 2024.Solomon Islands.*
[244] ASPI (Australian Strategic Policy Institute). 2022. Singh, Shailendra. "Marshall Islands
[245] Carreon, Tan, and Stoakes, "Foreign Workers, Local Sponsors."
[246] OCCRP. 2023. "US Bans Entry to Marshall Islands Politicians Over China-Linked Bribery Scheme." December 12, 2023.
[247] Carreon, Tan, and Stoakes, "Foreign Workers, Local Sponsors."
[248] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, Regional Office for Southeast Asia and the Pacific, April 2025.
[249] Ibid.
[250] Lily Hay Newman and Matt Burgess, "The Pig Butchering Invasion Has Begun," *Wired*, September 30, 2024.

signals are emerging, and which governance conditions may allow small nodes to consolidate into more strategic threats. Criminal diffusion typically seeks environments characterized by uneven AML enforcement, opaque beneficial ownership regimes, informal protection markets, and limited investigative capacity.[251]

Over the past decade, China has significantly expanded development finance, commercial investment, and elite-level political relationships across Africa, Latin America, South Asia, and parts of the Middle East.[252] This report does not assume centralized CCP orchestration of criminal diffusion; rather, the concern is structural. Where governance preferences prioritize political control, elite revenue generation, or selective enforcement over transparency and rule of law – patterns documented elsewhere in this report – expanding CCP-linked commercial density may interact with criminal entrepreneurship in ways that lower detection risk and enable criminal convergence.[253]

The central analytic task in this section is therefore forward-looking but disciplined: to distinguish confirmed operational presence from recruitment pipelines and laundering corridors; to assess whether governance conditions reflect passive tolerance or capacity constraints; and to identify early warning indicators that criminal relocation is evolving into entrenched accommodation.

3.5.1 Regional Evidence Snapshot

East Africa

Open-source reporting does not yet provide official confirmation of large-scale, compound-based coercive operations operating within Kenya, Uganda, or Tanzania. However, reporting is emerging and uneven, and the absence of documented official cases should not be interpreted as absence of activity. There is currently no sustained investigative ecosystem systematically examining this issue in the region, creating a significant visibility gap that itself warrants caution.

What is documented with confidence is that East Africa has become a meaningful recruitment zone for the Southeast Asian scam industry. Kenyan, Ugandan, and Ethiopian nationals have been trafficked to scam compounds in Burma and Cambodia under fraudulent job offers.[254] This demonstrates diffusion of the labor pipeline, even if confirmed onshore compounds remain undocumented.

Structurally, East Africa presents enabling conditions for the rapid rise of convergent criminal activity, similar to that observed in Southeast Asia. Chinese commercial and infrastructure presence is substantial in multiple countries under Belt and Road–linked financing.[255] While this does not imply state involvement in criminal activity, it indicates established logistics and commercial networks that criminal

---

[251] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, Regional Office for Southeast Asia and the Pacific, April 2025.

[252] Malik et al., *Banking on the Belt and Road*.

[253] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, Regional Office for Southeast Asia and the Pacific, April 2025.

[254] Mark Kelliher and Carlos Mureithi, "'I Broke Completely': How Jobseekers from Africa Are Being Tricked into Slavery in Asia's Cyberscam Compounds," *The Guardian*, September 9, 2025.

[255] Ammar A. Malik, Bradley Parks, Brooke Russell, Joyce Jiahui Lin, Katherine Walsh, Kyra Solomon, Sheng Zhang, Thai-Binh Elston, and Seth Goodman, *Banking on the Belt and Road: Insights from a New Global Dataset of 13,427 Chinese Development Projects* (Williamsburg, VA: AidData at William & Mary, 2021), https://www.aiddata.org/publications/banking-on-the-belt-and-road.

actors can potentially exploit for cover, property acquisition, and fund movement—patterns observed in other regions.[256] Evidence of laundering infrastructure tied specifically to pig-butchering operations in East Africa remains thin. At present, the region reflects primarily recruitment diffusion and potential passive regulatory vulnerabilities rather than confirmed entrenched enablement.

West and Southern Africa

West Africa presents clearer documented operational presence. In December 2024, Nigerian authorities dismantled a Lagos-based fraud hub involving approximately 800 suspects, including 148 Chinese and 40 Filipino nationals, targeting North American and European victims through romance-investment scams.[257] This constitutes direct evidence of a large transnational fraud operation operating in the sub-region.

In Namibia, a 2024 Interpol-coordinated raid rescued 88 trafficked youths forced to conduct scam operations.[258] These cases confirm that both hybrid distributed models and coercive elements are present in parts of Africa.

Chinese development finance and commercial presence across parts of West and Southern Africa provide contextual infrastructure that may facilitate operational embedding. This remains a structural correlation rather than evidence of CCP direction.[259] In typological terms, available evidence in West Africa reflects criminal network activity operating within environments of uneven enforcement and possible passive tolerance, rather than documented strategic exploitation.

Latin America

The evidence in Latin America remains limited, but significant. In 2023, Peruvian authorities rescued 43 Malaysians trafficked to Lima and forced to conduct telecom fraud operations under coercive conditions.[260] This case demonstrates that compound-style coercive models have replicated outside Asia, albeit episodically.

Beyond Peru, reporting suggests distributed fraud teams and potential laundering corridors in Brazil and Mexico.[261] However, region-wide entrenched compound ecosystems have not been documented.

As in Africa, Chinese commercial and infrastructure engagement has expanded significantly across Latin America over the past decade.[262] These investments create legitimate economic integration but also provide commercial density, established networks, and real estate activity that can be opportunistically exploited by criminal actors.[263] Evidence of systemic relocation remains fragmentary, and reporting coverage is thin in several countries, limiting definitive conclusions. Current evidence most closely aligns

[256] Lily Hay Newman and Matt Burgess, "The Pig Butchering Invasion Has Begun," *Wired*, September 30, 2024.
[257] Isaac Anyaogu, "Almost 800 Arrested over Nigerian Crypto-Romance Scam," *Reuters*, December 16, 2024.
[258] INTERPOL, "INTERPOL Releases New Information on Globalization of Scam Centres," June 30, 2025.
[259] Malik et al., *Banking on the Belt and Road*.
[260] "Dozens of Malaysians Rescued in Peru after Being Trafficked to Commit Online Fraud," *The Guardian*, October 9, 2023, last modified October 10, 2023.
[261] INTERPOL, "INTERPOL Releases New Information on Globalization of Scam Centres," June 30, 2025.
[262] Malik et al., *Banking on the Belt and Road*, pp. 20, 24.
[263] Lily Hay Newman and Matt Burgess, "The Pig Butchering Invasion Has Begun," *Wired*, September 30, 2024.

with early-stage presence in permissive or capacity-constrained environments rather than demonstrable state-linked enablement.

South Asia: Sri Lanka

Sri Lanka represents one of the clearest emerging nodes outside Southeast Asia. In 2024, Sri Lankan police arrested at least 84 foreign nationals, including 54 Chinese citizens, operating online scam centers from rented properties and tourist facilities.[264] These operations appear to have involved foreign-led fraud teams, with reported links to Dubai and other regional nodes.

While widespread labor coercion within Sri Lanka has not yet been documented at the scale seen in Burma, the operational model clearly reflects transnational replication. Sri Lanka's economic crisis and weakened oversight environment likely created permissive conditions for such activity.[265] As in other regions, Chinese development and commercial engagement forms part of the broader enabling infrastructure context.[266] Available evidence supports criminal network relocation into a governance environment characterized by regulatory stress, rather than direct evidence of CCP strategic coordination.

3.5.2 Modalities, Governance Conditions, and Transferability

Across emerging regions, convergent organized criminal activity does not replicate uniformly. Instead, the particular form depends on local governance structures, elite incentives, and the density of CCP-linked commercial and political integration.

The compound-based coercive model – characterized by centralized facilities, forced labor, and restricted movement – has been confirmed in Namibia[267], Peru[268], Mexico[269], and UAE[270]. These cases most closely resemble the Southeast Asian template, though at a smaller scale. Where such facilities emerge in jurisdictions with expanding China-linked infrastructure projects, opaque real estate acquisitions, or unusually dense clusters of Chinese state-affiliated shell entities, the analytic question shifts from mere criminal relocation to whether local enforcement tolerance reflects passive capacity constraints or emerging instrumental accommodation.[271]

In West Africa and parts of South Asia, hybrid distributed fraud models appear more prevalent. In Nigeria and Zambia, foreign-led teams operated alongside local recruits in office-like settings or under

[264] Tamil Guardian, "Sri Lanka's Online Fraudsters – Dozens Arrests Amidst Growth in Fraud Activity on the Island," *Tamil Guardian*, August 5, 2024.
[265] Ibid.
[266] Malik et al., *Banking on the Belt and Road*.
[267] INTERPOL, "INTERPOL Releases New Information on Globalization of Scam Centres," June 30, 2025.
[268] U.S. Department of the Treasury, "Treasury Targets Terrorism and Timeshare Fraud in Mexico," press release, August 13, 2025.
[269] "Dozens of Malaysians Rescued in Peru after Being Trafficked to Commit Online Fraud," *The Guardian*, October 9, 2023, last modified October 10, 2023.
[270] Lily Hay Newman and Matt Burgess, "The Pig Butchering Invasion Has Begun," *Wired*, September 30, 2024.
[271] Malik et al., *Banking on the Belt and Road*.

front-company cover.[272][273][274] These arrangements reduce visibility and allow operations to embed within legitimate-seeming commercial environments. Where such entities operate within jurisdictions receiving substantial Chinese investment or where local elites maintain unusually close financial relationships with Chinese commercial actors, the potential exists for convergence between commercial protection networks and criminal facilitation.[275] Current evidence does not demonstrate systematic CCP strategic exploitation in these regions. However, patterns consistent with passive tolerance – uneven enforcement, limited beneficial ownership transparency, and reluctance to pursue politically sensitive foreign actors – are observable.

Laundering and cash-out expansion remains the most transferable element of the ecosystem. Dubai functions both as an operational node and a financial hub.[276] U.S. Treasury actions against laundering entities such as Huione Group demonstrate how scam proceeds traverse global financial rails far beyond Southeast Asia.[277] As CCP-linked financial and commercial integration deepens across Africa and Latin America, early signs of underground banking overlap or clustering of high-risk digital asset exchanges warrant scrutiny, particularly where regulatory responses appear selective or delayed.[278]

These modalities are enabled by recurring governance conditions: corruption and informal protection markets,[279] weak anti–money laundering enforcement, investor visa and special economic zone regimes,[280] informal value transfer systems, and political instability.[281] In typological terms, most emerging regions presently reflect passive tolerance or capacity-driven weakness rather than documented instrumentalization or strategic exploitation. The early warning concern is whether increasing profit flows, combined with expanding CCP-linked commercial presence, shift incentives toward deeper accommodation.

The transferability of the model therefore lies not merely in replicating compound structures, but in embedding fraud operations within governance environments where political alignment, elite incentives, and regulatory discretion intersect.

3.5.3 Early Warning Indicators

Early detection of escalation requires attention not only to generic fraud signals but to indicators of convergence between scam operations and CCP-linked commercial or political networks. Concentrated real estate acquisitions tied to opaque shell entities connected to Chinese state-affiliated business networks may signal preparation of centralized facilities. Similarly, sudden emergence of

---

[272] Noel Sichalwe, "22 Chinese Nationals Sentenced to Long Prison Terms in Zambia for Multinational Cybercrimes," *Associated Press*, June 7, 2024, https://apnews.com/article/zambia-chinese-nationals-jailed-cybercrimes-f0e1dec5c4a08a23c270c469f70f8557.
[273] "Nigeria Arrests Nearly 800 in Raid on Crypto Pig Butchering Hub," *Reuters*, December 16, 2024, https://www.reuters.com/technology/cybersecurity/nigeria-arrests-nearly-800-raid-crypto-pig-butchering-hub-2024-12-16/.
[274] "Chinese Nationals Convicted of Running Cybercrime Ring from Zambia," *TRT Afrika*, June 7, 2024, https://www.trtafrika.com/article/18171037.
[275] Malik et al., *Banking on the Belt and Road*.
[276] Lily Hay Newman and Matt Burgess, "The Pig Butchering Invasion Has Begun," *Wired*, September 30, 2024.
[277] Chainalysis, *2025 Crypto Crime Report* (New York: Chainalysis, February 2025), https://go.chainalysis.com/2025-Crypto-Crime-Report.html.
[278] Malik et al., *Banking on the Belt and Road*.
[279] United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, Regional Office for Southeast Asia and the Pacific, April 2025.
[280] Lily Hay Newman and Matt Burgess, "The Pig Butchering Invasion Has Begun," *Wired*, September 30, 2024.
[281] Chainalysis, *2026 Crypto Crime Report* (New York: Chainalysis, January 2026), https://www.chainalysis.com/blog/2026-crypto-money-laundering/.

foreign-staffed "IT services," digital marketing, or crypto-trading firms in jurisdictions with significant Chinese development finance footprints warrants examination, particularly where ownership structures intersect with politically exposed local partners.[282]

Financial indicators are equally important. A surge in suspicious activity reports tied to corridors linking emerging nodes with Southeast Asian or Chinese financial intermediaries signals potential laundering convergence.[283] Expansion of lightly regulated digital asset exchanges clustered around Chinese commercial zones should be assessed for underground banking overlap. Growth in gambling or high-yield investment enterprises in jurisdictions hosting major Chinese infrastructure projects may provide cover for online fraud and capital recycling.

The strategic inflection point occurs when such signals coincide with political protection, regulatory inaction, or elite economic entanglement. Accordingly, the central early warning question is not simply whether fraud factories or other forms of contemporary organized criminal activity are emerging, but whether governance incentives—shaped in part by expanding CCP-linked commercial integration—begin to align with protection, instrumentalization, or selective tolerance of convergent criminal activity.

3.5.4 Case-Distinct Impacts on U.S. Interests

The emerging-frontiers dynamic presents distinct strategic implications for U.S. interests beyond those addressed in Part I.B.

First, diffusion into jurisdictions with expanding CCP-linked commercial integration complicates sanctions architecture. When scam-linked financial flows intersect with CCP-connected infrastructure projects, special economic zones, or politically sensitive commercial partnerships, enforcement actions may carry broader diplomatic consequences.[284] This raises the cost of disruption and may deter aggressive action by local authorities.

Second, geographic diversification increases the complexity of financial intelligence collection. As laundering corridors extend through Africa, Latin America, and South Asia, U.S. agencies must navigate fragmented regulatory environments, limited beneficial ownership transparency, and uneven cooperation. Where enforcement discretion aligns with political incentives favoring PRC-linked commercial relationships, investigative access may narrow.

Third, diffusion increases the resilience of networks targeting U.S. victims. Rather than relying on a small number of identifiable hubs, operators can shift activity across mid-tier jurisdictions with limited scrutiny. This complicates asset recovery and extends investigative timelines.
The case-distinct impact is therefore not merely expanded fraud geography, but the potential entanglement of transnational scam operations with political economies shaped by CCP-linked investment and influence. Whether emerging nodes remain episodic or evolve into durable hubs will depend on how governance incentives respond as criminal revenues scale.

[282] Malik et al., *Banking on the Belt and Road*.
[283] Chainalysis, *2026 Crypto Crime Report*.
[284] Malik et al., *Banking on the Belt and Road*.

Part IV CROSS-CUTTING FINDINGS
How Scam Ecosystems Scale and Survive

Across Cambodia, Burma, the Philippines, Pacific Island states, and emerging nodes, the evidence does not point to a single command structure. It does, however, suggest a repeatable operating model: scam ecosystems scale where criminal opportunity, political protection, dual-use infrastructure, and shadow finance converge. This section synthesizes the recurring mechanisms visible across cases and then interprets their strategic implications.

A. Recurring Enablement Mechanisms

Crackdowns can displace crime rather than destroy it

One of the most consistent patterns across cases is enforcement displacement. Periodic domestic crackdowns in the PRC have coincided with outward migration of fraud operations into jurisdictions with weaker oversight. Domestic enforcement pressure does not eliminate demand for illicit profit; it alters geography.

Extraterritorial enforcement actions, particularly repatriations of Chinese nationals from Southeast Asia, have often been selective and interest-driven. They prioritize domestic political stability, social order, and reputational management within China, rather than dismantling entire offshore ecosystems. This dynamic can reduce visible harm at home while leaving foreign victims and host jurisdictions to absorb externalized costs.

In Cambodia, enforcement pressure has periodically reshaped, rather than eliminated, scam infrastructure. In Burma, shifts in posture have recalibrated which actors operate and under what protection, without immediately collapsing the underlying model. In emerging regions, reporting suggests that enforcement surges in Southeast Asia have coincided with experimentation in Africa, South Asia, and Latin America. While causal links must be inferred cautiously, the pattern of geographic adaptation following pressure is consistent.

The structural throughline is externalization: harm is displaced outward when domestic costs rise. Strategic consequences can therefore arise even in the absence of high-level intent.

Protection markets

Criminal ecosystems scale where protection markets lower operational risk. These markets vary in form.

In Cambodia, documented patterns of elite patronage, regulatory permissiveness, and selective enforcement created conditions in which large-scale scam compounds could operate with relative insulation. In Burma, militia-controlled territories functioned as franchised governance zones, monetizing protection in exchange for revenue. In Pacific microstates, governance fragility and limited institutional capacity create vulnerability to elite-level influence, even without confirmed large-scale compound presence.

These systems are not necessarily CCP-run structures. They are political environments in which enforcement risk is reduced for networks linked to PRC-originating actors. When criminal operators can anticipate selective intervention rather than systematic dismantlement, incentives favor scaling.

Protection need not take the form of overt collusion. It may manifest as non-enforcement, delayed intervention, licensing blind spots, or jurisdictional fragmentation. The consistent feature across contexts is insulation from sustained accountability.

Legitimate infrastructure can become criminal infrastructure

Infrastructure does not need to be criminal in origin to become criminally useful. Casino complexes, real estate developments, border enclaves, SEZs, telecommunications networks, and logistics corridors provide opportunity structures. In an unclassified briefing, State Department officials offered a concrete articulation of this mechanism: SEZs intended to import a "Chinese development model" often evolve into consolidated ecosystems of casinos, underground banking, and vice markets – functioning as laundering hubs and crime multipliers.[285] That description reinforces the idea that the built environment and regulatory containers often serve the enabling substrate for later convergent criminal activity.

In mature hubs, casino and real estate infrastructure have been repurposed for centralized scam compounds. In border regions, enclave-style governance has facilitated concentrated operations. Across regions, telecommunications infrastructure – bulk SIM access, spoofing capacity, satellite connectivity – enables industrial-scale fraud independent of physical geography.

BRI-adjacent development and broader PRC commercial expansion have expanded established networks, property acquisition, and logistical density across multiple regions. These investments are overwhelmingly licit. However, commercial concentration and elite-level connectivity can lower friction for criminal actors seeking cover, leasing space, or moving funds.

Infrastructure's relevance lies in its dual-use character. The same features that facilitate trade and investment – connectivity, regulatory incentives, commercial clustering – can facilitate organized fraud if oversight lags.

Shadow finance makes crime portable

Fraud operations depend on scalable financial extraction and laundering. Underground banking systems, over-the-counter crypto brokers, shell-company networks, and identity arbitrage provide the connective tissue.

Across cases, scam proceeds traverse multiple jurisdictions before reaching consolidation points. Informal value transfer systems and crypto intermediaries reduce transparency. Citizenship and residency programs can provide identity flexibility. Corporate secrecy regimes complicate beneficial ownership tracing.

For U.S. exposure, the significance lies in intersection. Even when operational nodes remain offshore, laundering rails intersect with U.S.-connected financial institutions, digital platforms, and payment

[285] Unclassified briefing by U.S. Department of State officials to the House Select Committee on the Chinese Communist Party, March 2026, notes on file with the Committee.

systems. Geographic diffusion increases jurisdictional fragmentation, complicating asset recovery and sanctions enforcement. The portability of financial infrastructure may be more significant than the portability of physical compounds. As laundering corridors expand, resilience increases.

Selective enforcement manages visibility rather than eliminating the threat

PRC enforcement is often catalyzed by reputational risk and embarrassment dynamics—producing selective, visibility-oriented interventions. That logic is consistent with the notion of selective enforcement as risk management: it can lower visibility and political cost without dismantling underlying revenue structures.

Within this lens, crackdowns may target specific actors, regions, or moments of reputational sensitivity, while leaving underlying revenue-generating structures intact. Repatriations of Chinese nationals can reduce domestic political pressure without dismantling host-country protection markets. Diplomatic engagement may intensify following international scrutiny, then recalibrate once pressure subsides.

Post-Operation 1027 dynamics in Burma illustrate recalibration under geopolitical constraint. Enforcement pressure is mediated by border stability concerns and strategic interests. Similar recalibration patterns appear elsewhere.

Selective enforcement stabilizes the ecosystem by managing risk rather than eliminating it. It can reduce visibility while preserving underlying economic logic.

B. Governance and the Expansion of a CCP-Linked Distributed Criminal Ecosystem

The spread of scam networks is best understood as a governance problem. These networks scale where enforcement is selective, political protection is available, and opaque capital can buy influence.

The phenomenon has emerged most clearly in contexts heavily influenced by the PRC. The ecosystems documented in this report operate within governance environments characterized by opacity, centralized authority, patronage networks, and the instrumental use of coercion – features that resemble the CCP's own governance model and create conditions in which CCP-linked actors can operate with unusual advantage.

This creates a strategic disadvantage for the United States and its partners. U.S. influence depends heavily on transparency, accountable institutions, and rule-based cooperation. Scam ecosystems weaken those conditions. As they spread, they do not merely produce crime; they reshape the operating environment in ways that make U.S. policy harder to execute.

PART V. CONCLUSION

Foreign scam compounds began as a distant problem for many Americans: overseas fraud operations, hidden behind borders, shell companies, and digital platforms. They are no longer distant. They steal from U.S. citizens, rely on trafficked workers, exploit American technology and financial infrastructure, and strengthen criminalized political economies in regions central to U.S. economic and security strategy.

The Select Committee does not conclude that Beijing centrally commands this ecosystem. The more durable problem is that PRC-origin criminal networks and CCP-linked actors have repeatedly benefited from systems of selective enforcement, political protection, illicit finance, and opaque infrastructure.

The United States should not treat this problem singularly as consumer fraud, human trafficking, cybercrime, or great power competition. It is all of these at once. The appropriate response is not a sprawling regulatory agenda, but a focused national-security framework that raises the costs of foreign protection networks, strengthens interagency coordination, supports partner resilience, and ensures that critical private sector infrastructure does not continue to accelerate transnational criminal activity with little friction.

Congress cannot eliminate every scam compound by statute, nor can it eliminate all criminal misuse of global infrastructure. But it can help ensure that scam ecosystems face higher costs, fewer safe havens, stronger financial pressure, better interagency targeting, and more resilient partner states.

Distributed criminal ecosystems require distributed resilience. That resilience must combine law enforcement, financial pressure, diplomacy, governance support, private sector coordination, allied action, and clear-eyed engagement with the PRC where tactical cooperation is possible. Anything narrower will leave Americans exposed and the underlying ecosystem intact.

PART VI. POLICY RECOMMENDATIONS

1. Pass H.R. 5490 and synchronize it with the Cornyn-Shaheen SCAM Act. Congress should bring H.R. 5490, the Dismantle Foreign Scam Syndicates Act, to a floor vote and work to further synchronize it with the Cornyn-Shaheen Senate equivalent, S. 2950, the Scam Compound Accountability and Mobilization Act, which passed the Senate in December 2025. H.R. 5490 would establish an interagency task force to lead a whole-of-government effort against transnational scam syndicates operating large-scale scam compounds fueled by human trafficking for forced criminality. The Senate-passed SCAM Act similarly seeks to create a comprehensive response to foreign cyber scams, forced criminality, and fraud schemes targeting Americans. Together, these bills provide the clearest legislative foundation for treating foreign scam compounds as a strategic economic and national security threat to Americans, not merely as isolated overseas fraud operations. There is a core bipartisan consensus: scam compounds are transnational criminal enterprises that exploit forced labor, target U.S. citizens, and require sustained interagency action.

2. Establish sustained interagency coordination as the backbone of the U.S. response. Congress should ensure that new strategies and task forces are neither symbolic nor statutorily fragile. The threat cuts across the jurisdictions of DOJ, Treasury, State, DHS, FBI, FinCEN, the Intelligence Community, and U.S. embassies in affected regions. No single agency has the full map: law enforcement sees cases, Treasury sees financial flows, State sees partner-government constraints, DHS sees immigration and domestic penetration, and the Intelligence Community sees strategic context. Congress should therefore require regular interagency assessments of scam-compound ecosystems, laundering corridors, elite protection networks, and emerging geographic displacement. The objective should be a persistent operating picture: where compounds are located, who protects them, how proceeds move, which foreign officials enable them, how and where trafficking victims are recruited, and where networks are likely to relocate under pressure.

3. Increase pressure on foreign officials, business elites, and criminal facilitators who protect scam ecosystems. Scam economies flourish where criminal actors enjoy political insulation. Congress should encourage the executive branch to make fuller use of existing sanctions, visa restriction, anti-money laundering, and anti-corruption authorities against foreign officials, business elites, militia leaders, and financial facilitators credibly linked to trafficking-enabled scam operations. This recommendation does not need to create new sanctions architecture or dictate individual designations. Congress should press the executive branch to prioritize elite accountability, especially where scam compounds operate openly, rely on state-aligned armed protection, or generate rents for politically connected actors.

4. Support governance resilience in vulnerable partner states as a counterweight to criminalized CCP-influenced governance. Governance strengthening should be viewed as a core counter-crime and counter-influence tool. Scam ecosystems expand where rule-of-law institutions are weak, enforcement is selective, beneficial ownership is opaque, and political elites can monetize illicit capital. These are also conditions in which CCP-linked actors and PRC-origin TCOs can thrive. The United States' support should prioritize

independent journalism, civil society documentation, anti-corruption institutions, beneficial ownership transparency, financial intelligence capacity, victim protection, and local investigative capacity. In strategically sensitive environments, including Pacific Island states, small investments in transparency and institutional resilience may prevent criminal footholds from becoming long-term strategic vulnerabilities. This should not be framed as generic democracy assistance, but as a practical buffer against criminal governance and malign influence to protect U.S. national security interests.

5. Build an allied and regional coalition to prevent displacement and diffusion. Scam ecosystems adapt quickly. Pressure in Cambodia, Burma, or the Philippines can push operators into new jurisdictions in the Pacific, South Asia, Africa, Latin America, and the Middle East. The U.S. government should coordinate with key partners – including Australia, Japan, South Korea, Singapore, the United Kingdom, the European Union, and affected ASEAN states – to share intelligence, align sanctions and visa restrictions, monitor emerging nodes, and support cross-border victim rescue and evidence collection. The goal should be to prevent a whack-a-mole cycle in which enforcement in one jurisdiction merely relocates the problem elsewhere. A coalition-based approach would also reduce opportunities for corrupt or permissive states to play major powers against one another or quietly absorb displaced criminal capital.

6. Engage private sector infrastructure as a national-security partner. Scam ecosystems depend on private infrastructure: financial institutions, digital asset exchanges, advertising systems, messaging platforms, telecom networks, cloud services, and satellite connectivity. The U.S. government should therefore encourage structured public-private information sharing, typology development, rapid reporting channels, and voluntary or risk-based guardrails at critical chokepoints. The core principle is simple: if foreign scam networks use legitimate platforms and financial systems to industrialize victimization, the United States needs better coordination with the companies that operate those systems.

7. Mediate expectations for tactical cooperation with the PRC. The U.S. government should pursue tactical law enforcement cooperation with the PRC where it produces concrete, verifiable gains for U.S. citizens, trafficking victims, and partner governments. If PRC authorities are willing to share information, assist victim rescue, disrupt particular compounds, or support action against identifiable scam networks, the United States should not reject such cooperation on principle. At the same time, we should be clear-eyed about the limits of such cooperation. Beijing is most likely to offer highly public but token collaboration in the lead-up to major convenings[286] and/or when criminal activity threatens Chinese citizens, damages China's international reputation, destabilizes border regions, or creates diplomatic costs. The fentanyl experience offers a useful reference point: discrete enforcement cooperation can produce tactical gains while leaving deeper strategic incentives unresolved. The appropriate U.S. posture is therefore to welcome cooperation where verifiable, but not to substitute that cooperation for continued pressure on protection networks, independent intelligence collection, allied coordination, and a broader strategy designed around misaligned incentives and selective enforcement.

[286] https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting

Appendix: Chinese SOE Construction and Prince Group

Chinese corporate disclosures confirm that major Prince Group assets in Cambodia – including its Phnom Penh headquarters and the Sihanoukville Prince IT Tower – were constructed by China Construction Fourth Engineering Division (CSCEC Fourth Bureau), a subsidiary of the central SOE China State Construction Engineering Corporation (CSCEC).[287][288][289] These projects were later promoted as high-quality overseas engineering achievements, including receipt of the China Construction Engineering Luban Prize (Overseas), and framed within broader narratives of Chinese overseas development and cooperation.[290][291]

At the same time, Chinese judicial records show that Prince-linked entities and their principal, Chen Zhi (陈志), were involved in multiple civil and commercial disputes dating to the mid-2010s, including contract, debt, and liability cases.[292] Many of these cases precede or overlap with the 2017–2019 period during which these projects were developed. While not evidence of top-down PRC state criminality, they indicate that relevant risk signals were present within China's own systems prior to or during SOE engagement.

This juxtaposition reflects a broader pattern: risk indicators may exist but are not always disqualifying. For large Chinese SOEs operating overseas, project selection is shaped not only by risk, but by commercial opportunity, speed, and expansion priorities. In such environments, high-risk counterparties can remain viable partners, particularly where they provide access to land, regulatory pathways, or political networks.

Even absent direct involvement in illicit activities, SOE-built infrastructure can contribute to enabling conditions. Large-scale developments may later be repurposed within high-risk ecosystems where governance is weak, while association with a central SOE can confer legitimacy and reduce early scrutiny. In parallel, corporate materials framing these projects as part of China–Cambodia cooperation and "Maritime Silk Road" engagement further reinforce their political and symbolic significance.[293]

Consistent with this report's broader findings, these dynamics do not require centralized direction. Rather, they reflect enablement by effect: the alignment of incentives, permissive environments, and selective screening can produce outcomes that facilitate the growth of high-risk economic systems.

---

[287] 中国建筑第四工程局, "柬埔寨西港太子IT大厦项目成功中标," March 2018, http://4b1.cscec.com/xwzx/qyyw/201803/3155295.html

[288] Glofang, "柬埔寨西港太子IT大厦工程举行封顶仪式," December 28, 2018, http://www.glofang.com/news/show/102152/

[289] 中国建筑第四工程局, "太子中央广场、东景苑项目进展," October 2019, http://4cd.cscec.com/xwzx/qyyw/201910/2978883.html

[290] China Daily, "Overseas Projects Win Luban Prize," April 14, 2021, https://caijing.chinadaily.com.cn/a/202104/14/WS6076a7afa3101e7ce974926e.html

[291] 国务院国资委 (SASAC), "中国建筑海外工程展示中国质量," http://www.sasac.gov.cn/n2588025/n13790238/n16406218/c29125120/content.html ; 中国建筑第四工程局 WeChat posts (2019), archived screenshots describing Maritime Silk Road forum at Prince HQ

[292] 裁判文书网 (China Judgments Online), https://wenshu.court.gov.cn/ ; corroborated via Tianyancha (https://www.tianyancha.com) and Qichacha (https://www.qcc.com)

[293] 国务院国资委 (SASAC), "中国建筑海外工程展示中国质量," http://www.sasac.gov.cn/n2588025/n13790238/n16406218/c29125120/content.html ; 中国建筑第四工程局 WeChat posts (2019), archived screenshots describing Maritime Silk Road forum at Prince HQ

In sum, a central Chinese SOE subsidiary played a key role in building Prince Group's Cambodian real estate platform, even as risk signals existed within China's domestic system, illustrating how state-linked commercial activity can intersect with high-risk ecosystems without explicit coordination.