International Cybersecurity Law: Addressing Cross-Border Cybercrime and Cyber Warfare — With Special Focus on the Cambodia Cyber Scam Complex

Rudra Dev Singh
Rajiv Gandhi Institute of In Technology and Management, Bhopal, MP, India
singhrdsatna@rediffmail.com

Cybersecurity Law and Policy Review
Volume 1, Issue 1 | 2025 | https://clprj.com/journal/index

Abstract

Cross-border cybercrime has emerged as one of the defining legal and humanitarian challenges of the twenty-first century, exposing the structural inadequacy of a world legal order premised on territorial sovereignty to govern threats that are by nature transnational, anonymous, and technologically dynamic. This article examines the international legal framework governing cross-border cybercrime and cyber warfare, with sustained attention to the Cambodia cyber scam complex — a system of industrialised, state-tolerated online fraud and human trafficking that has victimised hundreds of thousands of individuals across Asia, Africa, and beyond, and that represents perhaps the most acute contemporary illustration of the governance gaps in international cybercrime law. Drawing on international criminal law, the law of state responsibility, human rights law, and comparative domestic criminal law, the article analyses the legal dimensions of the Cambodia scam phenomenon: the criminal enterprises that operate scam compounds along Cambodia's borders; the complicity of local governance structures; the transnational money laundering ecosystems that process the proceeds; the victimisation of trafficked workers forced to perpetrate fraud; and the inadequate response of the international legal community. The article then situates the Cambodia case within the broader framework of international cybersecurity law, examining the Budapest Convention regime, the emerging United Nations Cybercrime Convention, the law governing state-sponsored cyber operations, and the enforcement gaps that allow cross-border cybercrime to flourish with virtual impunity.

Keywords: *Cambodia cyber scam; cross-border cybercrime; international cybersecurity law; human trafficking; pig butchering; Budapest Convention; UN Cybercrime Convention; state responsibility; mutual legal assistance; cryptocurrency fraud*

1. INTRODUCTION

In 2023, the United Nations Office on Drugs and Crime (UNODC) estimated that criminal enterprises operating from scam compounds in Cambodia, Myanmar, Laos, and neighbouring countries were generating annual revenues in the range of thirty to forty billion United States dollars — a figure exceeding the gross domestic product of many of the states whose citizens they victimise. Behind this staggering statistic lies a human catastrophe of proportions that international law has been conspicuously slow to address: hundreds of thousands of workers, many trafficked under false pretences from China,

Taiwan, Vietnam, India, the Philippines, Indonesia, Thailand, and dozens of other countries across Asia and Africa, imprisoned in fortified compounds and compelled on pain of violence to perpetrate sophisticated online fraud against victims worldwide. The Cambodia cyber scam complex — the geographic and operational epicentre of this phenomenon, concentrated in the border zones of Bavet, Sihanoukville, Poipet, and Koh Kong — represents simultaneously a humanitarian emergency, an organised crime crisis, and a fundamental failure of international cybersecurity law and governance.

The Cambodia scam complex did not emerge in a vacuum. Its growth was enabled by the intersection of several structural factors: the rapid proliferation of digital payment infrastructure and social media platforms that provide both the tools and the target population for online fraud; the availability of jurisdictional safe havens in weakly governed border zones where local officials are complicit in or directly profitable from scam operations; the development of sophisticated money laundering ecosystems — centred on cryptocurrency and informal value transfer systems — that move and launder fraud proceeds with a speed and opacity that traditional financial intelligence tools struggle to match; and the deep deficiencies of the international legal framework governing cross-border cybercrime, which relies on voluntary cooperation between states whose interests are often misaligned with effective enforcement.

2. THE CAMBODIA CYBER SCAM COMPLEX: ORIGINS, STRUCTURE, AND OPERATION

2.1 Origins and Development

The origins of the Cambodia cyber scam complex lie in the confluence of three developments during the period 2019 to 2021. First, the COVID-19 pandemic devastated Cambodia's casino and tourism industry — which had attracted substantial Chinese investment and a large expatriate Chinese criminal ecosystem into the country — and displaced the criminal networks that had established themselves in Cambodia's Special Economic Zones (SEZs) toward new revenue streams that could operate despite border closures. Second, Chinese law enforcement's sustained crackdown on online gambling and fraud operations within China drove criminal operators offshore, to jurisdictions with weaker rule of law and more accommodating local power structures. Third, the explosive growth of social media platforms, dating applications, and cryptocurrency exchanges provided both the communication channels and the payment infrastructure for sophisticated online fraud at global scale.

The most prevalent fraud typology associated with the Cambodia scam complex — and now prevalent across the broader Southeast Asian scam ecosystem — is known variously as 'pig butchering' (shā zhū pán in Chinese, a term used by the criminal operators themselves), romance investment fraud, or confidence investment fraud. The methodology is deceptively simple in concept but operationally sophisticated: fraudsters cultivate online relationships with victims — typically through dating applications, social media platforms, or messaging applications — over weeks or months, building trust and affection before introducing the victim to what appears to be a highly profitable cryptocurrency or foreign exchange investment opportunity. The fraudulent investment platform, created and

controlled by the criminal enterprise, shows fictitious gains that encourage victims to invest progressively larger sums before the platform suddenly becomes inaccessible and all invested funds are stolen. Victims frequently suffer devastating financial losses — commonly of tens or hundreds of thousands of dollars — and the psychological trauma of simultaneous financial ruin and romantic betrayal.

2.2 Operational Structure of the Scam Compounds

The Cambodia cyber scam complex operates through a network of fortified compounds, predominantly located in border Special Economic Zones and coastal areas with weak state presence, that function as purpose-built fraud factories. These compounds — some of which occupy multiple city blocks and house thousands of workers — are typically owned or controlled by criminal networks with connections to Chinese organised crime, operating through layers of shell companies and local proxies that provide a degree of legal insulation for the ultimate beneficial owners. The compounds are equipped with the full technological infrastructure required for industrial-scale online fraud: high-bandwidth internet connectivity, banks of computers and mobile phones, scripting and training systems for fraud personnel, and cryptocurrency processing infrastructure for handling the proceeds.

The organisational structure within compounds mirrors that of legitimate business enterprises, with hierarchical management, performance targets, specialist departments (for victim cultivation, fraudulent investment platform management, cryptocurrency withdrawal processing, and technical support), and elaborate incentive and punishment systems. Workers who meet fraud targets may receive bonuses; those who fail to meet targets, attempt to escape, or resist participation in fraud operations face severe penalties including physical violence, food and sleep deprivation, debt bondage through the imposition of fees for 'recruitment', accommodation, and 'training', sale to other compounds, and in some documented cases, torture and killing.

2.3 The Human Trafficking Dimension

The workforce of the scam compounds is recruited and maintained through human trafficking on a massive scale. Workers are typically recruited through fraudulent job advertisements on social media platforms and messaging applications, offering attractive salaries for customer service, data entry, translation, or hospitality work in Southeast Asia. Victims travel — often paying their own travel costs — to Cambodia or neighbouring countries, where they are met by recruiters who transport them to the compounds. Upon arrival, their passports and identification documents are confiscated, they are informed of fabricated 'debts' for their recruitment and accommodation, and they are compelled under threat of violence to participate in fraud operations.

The human rights situation within the scam compounds has been extensively documented by investigative journalists, human rights organisations including Human Rights Watch and Fortify Rights, the UNODC, and diplomatic and consular services of source countries. Documentation includes accounts of systematic physical abuse, torture, forced labour, sexual violence, unlawful detention, denial of medical care, and obstruction of consular access. The scale of trafficking into scam compounds — with UNODC estimates suggesting that hundreds of thousands of people may be currently held in compounds across Cambodia, Myanmar, Laos, and neighbouring countries — constitutes one of the largest human trafficking crises in the contemporary world.

2.4 The Money Laundering Ecosystem

The proceeds of scam compound fraud operations flow through a sophisticated money laundering ecosystem that exploits the speed, pseudonymity, and global accessibility of cryptocurrency infrastructure combined with informal value transfer networks rooted in the Chinese diaspora and regional banking systems. Victim funds are typically directed initially into cryptocurrency wallets controlled by the criminal enterprise, frequently through fraudulent exchange platforms that appear to be legitimate trading venues. The cryptocurrency is then moved through multiple layers of wallets, mixing services, and cross-chain bridges designed to obscure the origin and beneficial ownership of the funds before being converted to fiat currency through exchanges with inadequate anti-money laundering controls, over-the-counter brokers operating outside regulated financial systems, or through the purchase and sale of real estate, luxury goods, and other high-value assets in jurisdictions with weak property purchase transparency requirements.

3. THE INTERNATIONAL LEGAL FRAMEWORK FOR CROSS-BORDER CYBERCRIME

3.1 The Budapest Convention on Cybercrime

The Council of Europe's Convention on Cybercrime, concluded in Budapest in 2001 and entered into force in 2004, remains the principal binding multilateral instrument governing international cooperation in the investigation and prosecution of cybercrime. The Budapest Convention establishes a framework of substantive criminal law obligations — requiring states parties to criminalise a range of computer-related offences including illegal access, data interference, computer fraud, and child sexual abuse material — and a comprehensive set of procedural cooperation mechanisms, including expedited preservation of electronic evidence, mutual legal assistance, and extradition provisions. The Convention has achieved comparatively wide ratification for a Council of Europe instrument, with approximately sixty-eight states parties as of 2025, including the United States, Japan, Australia, Canada, and many other non-European states.

However, the Budapest Convention's applicability to the Cambodia scam complex is substantially constrained by several structural limitations. Cambodia is not a party to the Budapest Convention and has not acceded to its framework, meaning that the expedited evidence preservation and mutual legal assistance provisions that would most directly facilitate investigation and prosecution of scam compound operators are not available as against Cambodian authorities. The Convention's mutual legal assistance provisions, even between states parties, have proven slow and bureaucratically cumbersome in practice — a deficiency particularly acute in the context of cybercrime investigations where evidence is volatile and perpetrators can rapidly relocate operations and assets across jurisdictional borders. The Second Additional Protocol to the Convention, which provides for more direct cooperation mechanisms and expedited evidence disclosure, has not yet achieved the ratification levels required to address these limitations at scale.

The substantive criminal law framework established by the Budapest Convention addresses computer fraud in general terms but does not specifically address the industrial-scale organised crime model exemplified by the Cambodia scam complex. The Convention's

focus on individual computer-related offences, rather than on the criminal enterprise structures through which organised cybercrime operates, means that it provides limited tools for the prosecution of the organising and directing tier of the scam compound hierarchy — those who establish, fund, manage, and profit from the compounds without personally executing individual fraud transactions. The application of organised crime frameworks — including the UN Convention Against Transnational Organised Crime (UNTOC) and its Protocols — to scam compound operators alongside the Budapest Convention framework represents a more legally adequate approach to the prosecution of compound leadership.

3.2 The UN Cybercrime Convention: Promise and Controversy

After years of debate in which a deeply polarised international community struggled to reach consensus on whether a new global cybercrime treaty was necessary, desirable, or achievable, the United Nations General Assembly adopted the United Nations Convention Against Cybercrime in December 2024. The Convention, negotiated over six years through an Ad Hoc Committee established by General Assembly Resolution 74/247, represents the first global multilateral cybercrime treaty and has the potential to significantly extend the geographic reach of international cybercrime cooperation beyond the Budapest Convention's membership — most critically, it has the prospect of including China, Russia, and other states that declined to accede to the Budapest framework.

However, the UN Cybercrime Convention has been the subject of sustained criticism from civil society organisations, technology companies, and a number of democratic governments who argue that its broad scope, weak human rights safeguards, and the cooperative mechanisms it establishes could be weaponised by authoritarian states to criminalise legitimate online expression and to compel democratic states to cooperate in the investigation of political dissidents, journalists, and human rights defenders under the guise of cybercrime enforcement. These concerns are not theoretical: the Convention's substantive criminal law provisions, as adopted, go substantially beyond computer-specific offences to encompass a broad range of 'crimes using ICT' that could be interpreted to capture forms of expression that are protected under international human rights law in democratic jurisdictions.

From the perspective of the Cambodia scam complex, the UN Cybercrime Convention's most significant potential contribution — and its most significant limitation — both relate to the possibility of bringing China into a binding international cybercrime cooperation framework. Chinese nationals constitute the largest single category of both perpetrators and victims of the Cambodia scam complex: the criminal enterprises operating the compounds are predominantly Chinese-owned and -managed, while the largest segment of trafficked workers and of fraud victims have historically been drawn from Chinese-speaking populations. Effective international law enforcement cooperation with Chinese authorities — who possess significant intelligence about the criminal networks involved and the capability to disrupt financial flows — is therefore essential to any comprehensive legal response to the Cambodia phenomenon. Whether the UN Cybercrime Convention will provide a functional framework for such cooperation, or will be selectively invoked in ways that protect Chinese criminal interests while targeting political adversaries, remains to be seen.

4. STATE RESPONSIBILITY AND THE CAMBODIA CYBER SCAM COMPLEX

4.1 The Law of State Responsibility Applied to Cybercrime Toleration

The Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), adopted by the International Law Commission in 2001, codify the customary international law framework for attributing internationally wrongful acts to states and determining the legal consequences of such attribution. Under the ARSIWA framework, a state bears international responsibility for conduct that is attributable to it and that constitutes a breach of an international obligation. The central question for the Cambodia case is whether the persistent failure of Cambodian state authorities to prevent, investigate, and prosecute scam compound operations — and, more seriously, the substantial evidence of direct involvement and facilitation by Cambodian officials — constitutes conduct attributable to Cambodia and breaching international obligations binding upon it.

The evidence of Cambodian official involvement in the scam compound ecosystem takes several forms. Investigative journalism and diplomatic reporting have documented the involvement of Cambodian military and police figures in providing security and logistical support to scam compounds, in facilitating the recruitment and transport of trafficked workers through official border crossing points, and in suppressing escapes and investigations. Senior political figures with connections to the ruling Cambodian People's Party have been linked through corporate and financial records to entities with interests in properties used as scam compounds. The UNODC's 2023 report on the Southeast Asia cybercrime landscape explicitly described the scam compound phenomenon as operating with 'elite protection' from elements of the Cambodian state.

Under the ARSIWA, conduct of state organs (including military, police, and border officials) is directly attributable to the state. The involvement of Cambodian state actors in facilitating scam compound operations therefore appears to satisfy the attribution requirement for state responsibility. The breach of international obligation requirement is satisfied by Cambodia's obligations under UNTOC and its Trafficking in Persons Protocol — both of which require active investigation and prosecution of trafficking offences — and potentially under customary international human rights law obligations requiring states to prevent, investigate, and remedy serious human rights violations committed on their territory. Whether Cambodia's conduct rises to the threshold of an internationally wrongful act — rather than merely inadequate implementation of treaty obligations — is a legal question whose answer depends on the degree to which Cambodia's failures are attributable to inability rather than unwillingness, a distinction that the evidence of active facilitation by state actors makes increasingly difficult to sustain.

4.2 Consequences and Enforcement Challenges

The establishment of Cambodia's international responsibility for the scam compound phenomenon would, under the ARSIWA framework, give rise to obligations of cessation, non-repetition, and reparation. In practice, however, the enforcement of state responsibility in the cybercrime context faces formidable structural challenges. The International Court of Justice, as the principal judicial organ for resolving disputes between states under international law, requires either a special agreement between the disputing states or the existence of a compromissory clause in the relevant treaty granting the Court jurisdiction

— and neither condition is readily satisfied with respect to Cambodia's UNTOC obligations. The political and diplomatic mechanisms through which state responsibility is enforced — bilateral representations, multilateral pressure, sanctions — operate slowly and face the well-documented limitations of applying coercive pressure to states with alternative sources of political and economic support. Cambodia's close relationship with China, which has been reluctant to apply pressure on the Cambodian government over scam compound issues despite the predominance of Chinese nationals among both perpetrators and victims, significantly limits the international community's leverage.

The targeted sanctions regimes maintained by the United States, European Union, and United Kingdom — which authorise the designation of individuals and entities involved in human rights abuses, corruption, and organised crime — provide a more immediately operational tool for holding specific Cambodian officials accountable. The United States has made limited use of its Global Magnitsky Act authority to sanction Cambodian officials implicated in the scam compound ecosystem, and more systematic application of targeted financial sanctions and travel bans against senior officials with documented involvement in the protection of scam operations would increase the personal cost of complicity and potentially alter the incentive structures that currently sustain official protection of the compounds.

5. HUMAN RIGHTS LAW AND THE PROTECTION OF TRAFFICKED CYBER-FRAUD WORKERS

5.1 The Legal Status of Trafficked Scam Workers

One of the most legally complex and humanistically challenging dimensions of the Cambodia scam complex is the status of the workers who are compelled to perpetrate fraud within the compounds. These individuals are simultaneously victims — of human trafficking, forced labour, torture, unlawful detention, and multiple other serious human rights violations — and perpetrators of serious criminal offences against fraud victims who may lose their life savings. The legal framework's treatment of this duality has profound implications for justice: a framework that prioritises the prosecution of all participants in fraud operations without adequately accounting for the coercive conditions under which many participated risks compounding the victimisation of trafficked workers; a framework that provides blanket immunity for participation in fraud denies justice to the financial victims whose losses may be equally devastating.

International trafficking law and human rights law are clear that persons who commit crimes under compulsion as a result of their trafficking and exploitation should not be held criminally responsible for those crimes — a principle sometimes described as the 'non-criminalisation principle' or 'non-punishment principle'. The Palermo Protocol does not explicitly codify this principle, but it has been articulated in the Council of Europe Convention on Action against Trafficking in Human Beings (Article 26), the EU Anti-Trafficking Directive (Article 8), and the UNODC Model Law Against Trafficking in Persons. The consistent position of international human rights bodies — including the Special Rapporteur on Trafficking in Persons — is that trafficked persons who commit offences as a direct result of their trafficking should not be penalised for those offences,

and that prosecutorial discretion should be exercised to reflect the coercive circumstances of participation in criminal activity.

5.2 Obligations of Source, Transit, and Destination States

The human rights dimensions of the Cambodia scam complex engage the obligations not only of Cambodia but also of the source countries from which workers are trafficked and the destination countries into which fraud proceeds flow. Source country governments bear obligations under international human rights and anti-trafficking law to protect their nationals from trafficking — including through awareness-raising, border screening, consular protection, and the prosecution of domestic recruitment networks that supply the compounds. The performance of source country governments in fulfilling these obligations has varied substantially: some governments have been proactive in warning their nationals, assisting with repatriation, and prosecuting domestic recruiters, while others have been slow to acknowledge the scale of the problem or have prioritised maintaining bilateral relations with Cambodia over the protection of their trafficked nationals.

Transit states — through whose territory workers are transported, often through normal border crossing points — bear obligations to screen migrants and intercept trafficking victims before they reach the compounds. The systematic exploitation of legitimate travel routes through Thailand and Vietnam as transit channels to scam compounds in Cambodia highlights the failure of transit state border management and screening systems to identify trafficking patterns that have become widely documented and publicly known.

Financial destination states — the jurisdictions into which fraud proceeds ultimately flow, and in which the real estate, luxury goods, and financial assets acquired with those proceeds are located — bear obligations under anti-money laundering and asset recovery frameworks to identify, freeze, and confiscate crime proceeds. The United States, Singapore, Hong Kong, the United Arab Emirates, and several European financial centres have been identified as destinations for proceeds of Cambodia scam compound fraud, and their fulfilment of anti-money laundering and asset recovery obligations is central to any comprehensive disruption of the scam compound financial model.

6. CROSS-BORDER CYBERCRIME AND THE LAW OF CYBER WARFARE

6.1 State-Tolerated Cybercrime as Economic Warfare

The scale and systematic character of the Cambodia cyber scam complex — and of the broader Southeast Asian scam ecosystem of which it forms part — raises questions that go beyond conventional cybercrime law to engage the frameworks governing hostile acts between states. The UNODC's estimate that criminal enterprises in the region generate thirty to forty billion dollars annually in fraud proceeds represents a flow of wealth from victim countries — predominantly China, Taiwan, the United States, and other relatively affluent nations — to the criminal networks and their state protectors that in aggregate constitutes a significant economic impact. Some analysts and governmental commentators have characterised state-tolerated industrialised cybercrime at this scale as a form of economic warfare, though this characterisation has not yet achieved formal legal recognition in international instruments or authoritative doctrinal analysis.

Under the framework of the Tallinn Manual 2.0 and the consensus positions of UN Groups of Governmental Experts on responsible state behaviour in cyberspace, a state that knowingly allows its territory to be used as a base for cyber operations against other states may bear responsibility for those operations where it has the capacity to prevent them and fails to do so. This 'due diligence' principle — drawn from the Trail Smelter arbitration and its progeny in general international law — has been applied by multiple authoritative analyses to the cyber context, implying that a state that is aware of cybercrime operations being conducted from its territory against foreign victims and that has the capacity to suppress those operations is under an obligation to do so. Cambodia's failure to suppress the scam compound operations despite documented awareness of their scale and character arguably engages this due diligence obligation, though the capacity caveat provides some legal insulation for a state that claims insufficient law enforcement resources to address the problem.

6.2 Jurisdictional Assertions and Enforcement in Cyberspace

The cross-border character of scam compound cybercrime — perpetrated from Cambodia against victims worldwide, using technical infrastructure that may be located in multiple jurisdictions, with proceeds flowing through financial systems across the globe — raises jurisdictional questions of considerable complexity. The traditional bases of criminal jurisdiction in international law — territoriality, nationality, passive personality, protective principle, and universality — each provide partial but incomplete coverage of scam compound operations from the perspective of any individual victim state. The victim state's passive personality jurisdiction over offences whose victims are its nationals is established under the law of most jurisdictions, but is difficult to exercise against perpetrators located in Cambodia without effective extradition or mutual legal assistance arrangements.

The United States' assertion of extraterritorial jurisdiction over money laundering offences involving US financial institutions or US-dollar-denominated transactions has proven a more practically effective tool in some cases, providing a basis for US law enforcement action against financial flows connected to scam compound operations even without the cooperation of Cambodian authorities. United States v. various asset forfeiture actions have targeted cryptocurrency holdings and financial accounts linked to scam compound proceeds, and the Department of Justice's KleptoCapture task force model — developed in the context of Russian oligarch asset recovery following the Ukraine invasion — provides an institutional template that could be adapted for systematic scam compound asset recovery.

7. NORMATIVE RECOMMENDATIONS FOR LEGAL REFORM

7.1 Strengthening the International Cybercrime Cooperation Framework

The most fundamental structural reform required to address the Cambodia scam complex — and the broader phenomenon of industrialised cross-border cybercrime operating from governance-weak jurisdictions — is the construction of a more effective and comprehensive international legal framework for cybercrime cooperation. This requires, first, the broadest possible ratification of the Budapest Convention and its Additional Protocols, including by Southeast Asian states currently outside the framework; second,

the effective implementation of the UN Cybercrime Convention in a manner that genuinely advances international cooperation against the Cambodia-model scam complex while incorporating robust human rights safeguards; and third, the development of specific international instruments addressing the organised criminal enterprise character of the scam compound phenomenon, going beyond the computer-offence-specific framework of the Budapest Convention to engage the full range of predicate offences involved.

Mutual legal assistance reform must be a central priority. The traditional MLAT framework — with its requirement for dual criminality, its reliance on central authority transmission, and its processing times measured in months or years — is wholly inadequate for cybercrime investigations that require rapid evidence preservation and real-time financial intelligence sharing. Emergency preservation orders, direct law enforcement-to-law enforcement communication channels for time-sensitive matters, and the streamlining of MLAT requests for cryptocurrency-related evidence should be advanced through both the Budapest Convention Second Additional Protocol framework and bilateral agreements among key partner states in the anti-scam coalition.

7.2 A Dedicated International Anti-Scam Coalition

The unique and unprecedented character of the industrial-scale scam compound phenomenon — combining cybercrime, human trafficking, money laundering, and state toleration in a configuration not anticipated by existing international legal instruments — makes a compelling case for the establishment of a dedicated international anti-scam coalition, analogous to the coalitions established to address piracy and foreign terrorist fighters. Such a coalition, operating under a mandate drawn from the UN Security Council, would coordinate the intelligence-sharing, law enforcement, diplomatic, financial, and legal assistance activities of participating states, provide a forum for the development of coordinated responses to state complicity in scam operations, and aggregate the political pressure necessary to produce genuine reform of enforcement in source and destination jurisdictions.

China's inclusion is essential: the predominance of Chinese criminal networks in the scam compound ecosystem, combined with China's unique leverage over the Cambodian government and its capacity to take action against the financial networks processing scam proceeds within Chinese financial infrastructure, means that an effective international response without Chinese participation would be materially incomplete. The development of a framework for Chinese cooperation that is sufficiently respectful of Chinese sovereignty concerns to be politically achievable while sufficiently robust to produce genuine law enforcement collaboration represents the central diplomatic challenge for the international response to the Cambodia scam complex.

7.3 Targeted Sanctions and Asset Recovery

Targeted sanctions regimes — applied to senior Cambodian officials with documented involvement in the protection of scam compound operations, to the beneficial owners and operators of major scam enterprises, and to the financial institutions and intermediaries that knowingly process scam proceeds — represent one of the most immediately actionable legal tools available to the international community.

Asset recovery — the tracing, freezing, and confiscation of scam proceeds wherever they are held — must be elevated to a central element of the anti-scam legal strategy. The proceeds of scam compound fraud are not merely the measure of criminal profit; they are the primary mechanism through which fraud victims suffer harm, and their recovery and restitution to victims should be the legal system's most direct response to that harm.

7.4 Human Rights Protections for Trafficked Scam Workers

The non-punishment principle for trafficked scam workers must be consistently and explicitly applied across all jurisdictions that receive returned nationals. Source country governments should adopt clear prosecutorial guidance implementing the non-punishment principle, establish specialised victim identification and support mechanisms for returned scam compound workers, and invest in psychological and economic rehabilitation programmes for survivors. The repatriation of trafficked nationals — which has been complicated in some cases by the unwillingness of Cambodian authorities to facilitate rescues and by the cost of ransom payments demanded by compound operators for the release of their workers — should be treated as a consular protection priority, with emergency funding mechanisms to support rescue operations and repatriation costs.

Survivor testimony — from individuals who have been held in and escaped from scam compounds — constitutes some of the most valuable intelligence available for the investigation and prosecution of compound operators. Witness protection frameworks, including resettlement options for survivors who face threats from criminal networks in their home countries, are an essential precondition for the effective use of survivor evidence in criminal proceedings. International cooperation in the development of such frameworks — including joint investigation teams that can pool survivor testimony from multiple jurisdictions to build comprehensive cases against compound leadership — should be a priority for the proposed anti-scam coalition.

7.5 Platform and Financial Sector Accountability

The Cambodia cyber scam complex could not operate at its current scale without the cooperation — witting or unwitting — of major digital platforms, social media networks, messaging applications, and financial infrastructure that provide the channels through which fraudsters recruit victims and through which scam proceeds are transferred and laundered. Legal frameworks must impose more robust obligations on these actors to detect and disrupt scam activity on their platforms and in their financial systems. This includes requirements for social media platforms to implement effective detection of fraud-related content and accounts; for messaging applications to provide law enforcement with timely access to evidence in cybercrime investigations; for cryptocurrency exchanges to implement more rigorous customer due diligence and transaction monitoring for patterns consistent with scam proceed laundering; and for correspondent banking networks to apply enhanced due diligence to transactions involving jurisdictions with documented scam compound activity.

The legal basis for platform accountability varies across jurisdictions. In the European Union, the Digital Services Act's provisions regarding illegal content and the obligations of very large online platforms provide a framework that can be interpreted to encompass scam-related fraud activity. In the United States, Section 230 of the Communications Decency Act has historically provided broad immunity to platforms for third-party content,

though the application of this immunity to fraud facilitation — rather than mere content hosting — has been the subject of increasing legal challenge. Regulatory action by financial supervisors under existing anti-money laundering frameworks, combined with targeted legislative reform to clarify platform liability for knowingly enabling fraud activity, represents the most achievable near-term avenue for engaging the platform and financial sectors more effectively in the anti-scam effort.

8. CONCLUSION

The Cambodia cyber scam complex is not merely a law enforcement problem to be resolved through the application of existing legal tools — it is a symptom of deep structural deficiencies in the international legal order's capacity to govern transnational threats that combine technological sophistication, organised crime, state complicity, human trafficking, and financial globalisation in ways that existing legal frameworks were not designed to address. The tens of billions of dollars in annual fraud proceeds, the hundreds of thousands of human beings trafficked into forced labour in fortified compounds, and the millions of victims worldwide who have suffered devastating financial and psychological harm together constitute a humanitarian crisis and a governance failure of the first order.

The legal analysis advanced in this article identifies multiple dimensions of the international legal framework's inadequacy: the geographic limitations of the Budapest Convention framework; the as-yet uncertain contribution of the UN Cybercrime Convention; the failure to apply UNTOC obligations effectively to the scam compound context; the underutilisation of state responsibility doctrine to hold Cambodia accountable for official complicity; the inconsistent application of the non-punishment principle to trafficked scam workers; and the absence of a dedicated international coordination mechanism capable of aggregating the political will, intelligence resources, and law enforcement capacity required for a comprehensive response.

REFERENCES

African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), adopted 27 June 2014, entered into force 8 June 2023.

Articles on Responsibility of States for Internationally Wrongful Acts, International Law Commission, 53rd session (2001), UN Doc A/56/10.

Budapest Convention on Cybercrime (Council of Europe), ETS No. 185, opened for signature 23 November 2001, entered into force 1 July 2004.

Council of Europe Convention on Action against Trafficking in Human Beings, CETS No. 197, opened for signature 16 May 2005, entered into force 1 February 2008.

EU Anti-Trafficking Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings.

EU Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022.

Federal Bureau of Investigation (FBI), '2023 Internet Crime Report' (FBI Internet Crime Complaint Center, 2024).

Financial Action Task Force (FATF), 'Cyber-Enabled Fraud' (FATF, 2023).

Fortify Rights, 'They Gave Us Phones and Forced Us to Work' (Fortify Rights, 2023).

Global Magnitsky Human Rights Accountability Act, 22 U.S.C. § 2656 note (2016).

Human Rights Watch, 'Online Scam Operations and Trafficking in Southeast Asia' (Human Rights Watch, 2023).

International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries' (ILC, 2001).

Interpol, 'Financial Crimes in Southeast Asia: Cyber-Enabled Scam Operations' (Interpol, 2023).

Palermo Protocol (UN Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children), supplementing the United Nations Convention Against Transnational Organised Crime, opened for signature 15 November 2000, entered into force 25 December 2003.

Rome Statute of the International Criminal Court, 2187 UNTS 90, opened for signature 17 July 1998, entered into force 1 July 2002.

Silverstein, K., 'Scam Inc.: How Cambodia Became the Global Capital of Cyber Fraud' (Vox, April 2024).

United Nations Convention Against Cybercrime, adopted by UN General Assembly Resolution 79/243, 24 December 2024.

United Nations Convention Against Transnational Organised Crime (UNTOC), 2225 UNTS 209, opened for signature 15 November 2000, entered into force 29 September 2003.

United Nations General Assembly Resolution 74/247, 'Countering the Use of Information and Communications Technologies for Criminal Purposes' (27 December 2019).

United Nations General Assembly, 'Report of the Special Rapporteur on Trafficking in Persons, Especially Women and Children', UN Doc A/HRC/53/28 (2023).

United Nations Office on Drugs and Crime (UNODC), 'Casinos, Cyber Fraud and Trafficking in Persons for Forced Criminality in Southeast Asia' (UNODC, 2023).

United Nations Office on Drugs and Crime (UNODC), 'Transnational Organised Crime in Southeast Asia: Evolution, Growth and Impact' (UNODC, 2024).

.