Revija za kriminalistiko in kriminologijo / Ljubljana 76 / 2025 / 4, 332–345

Scam Cities: Criminal Hubs in Transnational Cybercrime Networks

Sara Lilli[1], **Maria Vittoria Zucca**[2]

This research serves to explore the phenomenon of so–called "Scam Cities": urban or semi–urban hubs, primarily located in Southeast Asia, where criminal networks orchestrate large–scale cyber fraud through the exploitation of trafficked individuals subjected to forced labour. Often disguised as call centres or gambling operations, these compounds represent a convergence of cybercrime, human trafficking and transnational organized crime. Despite growing journalistic attention, the subject remains underexamined in legal and criminological literature. The study develops along two main axes. The first examines the "life cycle" of scam compounds, focusing on: 1) deceptive recruitment strategies; 2) organizational structures; 3) fraud schemes employed; and 4) illicit financial flows. The second provides responses across a temporal spectrum: 1) prevention, aimed at mitigating criminal risks and enhancing awareness; 2) enforcement, directed at identifying countermeasures and related legal lacunae; and 3) post–release support, addressing survivors' reintegration and legal recognition. By addressing these dimensions, the study aims to contribute to global discussions on scam compounds, deepen academic understanding of the phenomenon and provide insights to inform policy, legal frameworks and practical interventions.

Keywords: scam cities, digital slavery, transnational organized crime, human trafficking, cybercrime

UDC: 343.341

1 Introduction

The present study investigates the dynamics of so–called scam cities, framed within the scam–compound model – that is, industrial–scale cyber fraud – managed by organized criminal groups, involving workers held in conditions akin to modern (cyber) slavery. Located primarily in the borderlands between Thailand, Myanmar, Laos and Cambodia, these sites function as semi–autonomous urban enclaves that attract capital, labor and transnational illicit flows. Many observers portray them as a new iteration of the so–called "Golden Triangle" (Giordana & Morello, 2025; Laungaramsri, 2025), a region once notorious in the latter half of the twentieth century for narcotrafficking and frontier economies, which has now redirected its criminal infrastructures toward cyberspace and online frauds. It should be recognized, preliminarily, that these scam hubs did not suddenly materialize out of thin air (Franceschini et al., 2025), rather, they have "mushroomed" in parallel with geographic and socio–economic criminal facilitators (Hall et al., 2021), in a long trajectory of legal ambiguity and fragmented sovereignty, typical of the Mekong borderlands. In fact, in these areas, the absence of effective state control, pervasive impunity and corruption, the collusion between political elites and local armed groups and the persistent cross–border demand (e.g., gambling, prostitution or contraband goods) have produced economies that constantly oscillate between legality and illegality, formality and informality. Within this context, former hubs of narcotrafficking and gambling have progressively been reconverted into digital fraud centres, giving rise to criminal cities that combine material infrastructures (e.g., casinos and fortified residential complexes) with immaterial ones (e.g., online platforms and covert financial networks) (Franceschini et al., 2023; Lazarus et al., 2025). Online gambling, in particular, has played a central role in the rise of this illicit economy in Southeast Asia (Franceschini et al., 2025). As criminologist James Banks (2016) observes, the online gambling and scam sectors have been closely intertwined since the early days of the Internet, indeed, from the mid–1990s onward, gambling has been plagued by illegal operations, money laundering and fraud schemes. A decisive turning point occurred in the 2000s (Gore et al., 2022), when the Chinese authorities implemented regulations against domestic casinos, prohibiting gambling nationwide (with the exceptions of the Special Administrative Regions of Hong Kong and Macau). This policy forced many operators, often linked to organized crime networks, to shift their activities abroad in search of "more permissive" environments (Global Initiative Against Transnational

[1] Sara Lilli, Doctoral Student, Sant'Anna School of Advanced Studies (Pisa) and IMT School for Advanced Studies (Lucca), Italy. ORCID: 0009-0000-2796-3067. E-mail: sara.lilli@imtlucca.it

[2] Maria Vittoria Zucca, Doctoral Student, Sant'Anna School of Advanced Studies (Pisa) and IMT School for Advanced Studies (Lucca), Italy. ORCID: 0009-0004-0049-9611. E-mail: mariavittoria.zucca@imtlucca.it

Organized Crime, 2025). Southeast Asia offered such conditions, with the border between Mae Sot (Thailand) and Myawaddy (Myanmar) standing out as a paradigmatic case. The porous nature of this 1,500–mile frontier – characterized by mountainous terrain and multiple crossing points – has for decades facilitated the mobility of people and goods, with the Moei River, which marks part of the boundary, serving as a vital corridor of transit around which local economies and trade networks have long developed.

The borders between Thailand and Myanmar have never been rigidly defined nor unanimously recognized. This territorial ambiguity has enabled local armed groups – such as the Karen National Union (KNU), the Border Guard Forces (BGF) and the Democratic Karen Buddhist Army (DKBA) – to exercise direct control over the area, managing trade routes, imposing taxes and overseeing cross–border flows. The absence of consistent border governance produced a hybrid economic system in which both state and non–state actors shared resources, revenues and jurisdictions (Asia Foundation, 2025; Giordana & Morello, 2025). The roots of this scenario lie in the history of informal trade and smuggling that characterized Mae Sot/Myawaddy. Indeed, during the 1980s and 1990s, the local economy prospered as a transborder hub primarily based on agricultural products and consumer goods. Over time, informal trade networks expanded to include more lucrative commodities – such as timber, precious stones, counterfeit pharmaceuticals, and electronics – yielding rising profits. In this setting, both state officials (customs officers, military personnel) and non–state actors (ethnic armed groups, local businessmen) profited by imposing informal taxes and tolls, consolidating a parallel economy that transformed the border from a line of separation into a political and economic resource. A crucial step in the area's evolution toward its current criminal configuration was the development of cross–border gambling. In the 1990s and 2000s, enclaves such as Shwe Kokko (Karen State) and Laukkai (Kokang region) were authorized (or tacitly tolerated) in establishing casinos and resorts, catering primarily to Chinese and Thai clients coming from countries where gambling was banned. These enclaves functioned as genuine "grey zones of sovereignty" (Abraham & van Schendel, 2005), formally within the national territory, yet *de facto* semi–autonomous thanks to the protection of local elites, armed groups and complicit officials. Casinos, quickly becoming poles of attraction, also turned into multifunctional hubs of parallel economies, including prostitution, narcotics and the smuggling of precious goods. The construction of this economic and social infrastructure around gambling – made of resorts, residential towers, parallel payment systems and politico–military protection – laid the foundation for their later reconversion into scam compounds. The same logic of extraterritoriality that enabled the attraction of gamblers across borders has been repurposed, in more recent years, to host fraudulent call centres and online scam operations on a global scale. Scam cities therefore, do not represent a rupture but rather the mutation of a broader economic and geopolitical continuum: from agricultural smuggling in the 1980s, to gambling in the 1990s and 2000s, to contemporary digital criminality.

Over time, the entrenched presence of these parallel powers normalized the existence of grey economies, transforming the border into a resource to be exploited rather than a line of division. The expansion of Special Economic Zones (hereinafter SEZs) and the inflow of foreign capital, officially presented as drivers of modernization, have in practice provided new infrastructures and legal cover for illicit operations. Casinos, industrial parks and residential complexes built along the frontier have become spaces where licit and illicit capital intersect and where transnational criminal networks have consolidated durable strongholds (Asia foundation, 2025; Giordana & Morello, 2025). In this sense, the region's scam cities embody the outcome of a genuine "frontier ecosystem", in which the boundary between governance and crime is structurally blurred and where border porosity itself becomes the primary enabling factor of organized fraud.

This illicit industry generates tens of billions of dollars per year, with revenues from cyber scams in the Mekong estimated to equal approximately 40% of the combined formal gross domestic product (GDP) of Laos, Cambodia and Myanmar (USIP Senior Study Group on Transnational Organized Crime in Southeast Asia, 2024). With such staggering profits, it is little surprise that the model has spread beyond the region, with forced–labour scam centres now documented in the UAE, Montenegro, Peru and Namibia (Global Initiative Against Transnational Organized Crime, 2025).

The present analysis, however, confines its scope to the emergence and internal dynamics of scam cities in Southeast Asia.

2 Organizational, Operational and Financial Dimensions of Scam Compounds

The following sections will reconstruct, on the basis of sectoral reports and available sources, the "life cycle" of a scam city, namely the mechanisms that sustain its existence. The analysis will foreground: 1) the mechanisms of recruitment, 2) the organizational architecture of compounds and their division of labour, together with 3) the fraud schemes and 4) illicit financial circuits through which these hubs sustain and expand their transnational operations.

2.1 Recruitment Mechanisms and the Notion of "Cyber-victimhood"

To start, a 2023 report by the UN Office of the High Commissioner for Human Rights noted that "credible sources" estimated that at that time, at least 120,000 individuals were being held under conditions that forced them to participate in online scams in Myanmar, with another 100,000 in Cambodia (United Nations Human Rights Office of the High Commissioner, 2023). These estimates demonstrate the scale of the phenomenon, which is underpinned by recruitment and trafficking networks that are often complex to map, varying by country of origin and involving multiple actors such as recruiters, brokers and traffickers. In some cases, recruitment chains even collaborate with legitimate employment agencies, whereby individuals initially seeking lawful jobs – such as through Dubai–based agencies – are misled into participating in scam operations in Southeast Asia, with some agencies reportedly complicit and receiving payments from criminal networks (Humanity Research Consultancy, 2024).

On the other side of recruitment, equally complex in its boundaries and definition, lies the notion of the victim. Indeed, in reference to individuals sold, kidnapped, or trapped in the online scam industry, the term "cyber slave" has gradually been popularized in journalistic discourse. The term underscores the paradoxical condition of individuals who, while subjected to coercion and deprived of freedom, remain continuously connected to the digital environment – a juxtaposition that sets this form of exploitation apart from more "traditional" forms of slavery.

However, this conceptualization entails critical issues: 1) it risks portraying the phenomenon as unprecedented, thereby obscuring its continuities with established forms of modern slavery and forced labour, potentially marginalizing these

Table 1: Recruitment mechanisms

Strategy	Communication channels	Core features
Job adverts	Job–recruitment websites. Social media platforms (Facebook, Instagram, LinkedIn, Reddit). Instant–messaging apps (Telegram, Line, WeChat and QQ). Pop–up ads and banner ads (streaming, gaming sites, shady websites). Fake HR agency websites / cloned recruitment portals.	Vague job descriptions ("crypto investors", "engineers", "translators"). Promises of free food, housing and travel, with emphasis on "no fees". Language requirements (Chinese, English, others). High salaries vs. low skills required. Target: young adults (18–35). Locations tied to gambling/scam hubs.
«Structured» recruiters	Licensed recruitment agencies (some may be complicit in fraudulent schemes). Independent brokers operating remotely in source countries. Social media platforms (e.g., dating apps, online gaming communities). Peer–to–peer networks (friends, relatives or " hometown connections"). Direct, in–person recruitment through personal contacts or community ties.	Commissions earned per recruited individual, formal integration within scam compounds. Use of deception based on trust–building: i) posing as friends, colleagues, relatives, gaming teammates; ii) long–term grooming (weeks/months) before presenting job offer; iii) "pretending–to–be–rich" strategy (luxury lifestyle posts). Coercive mechanisms: victims told they cannot leave unless they recruit replacements. Company–sponsored logistics: flights, visas, work permits arranged.
«Opportunistic» recruiters	Friends, acquaintances and relatives (trusted social circles). Fellow townspeople or people sharing the same place of origin. Informal personal networks at workplaces or communities. In–person contact in daily life (restaurants, workplaces, local neighbourhoods).	Exploit pre–existing trust within social/family networks (offering seemingly safe or well–paid jobs). Payment per recruited person (sporadic, opportunistic or debt–based). Victims often unaware of risks; trust leads to deception and breakdown of societal trust near scam hubs. Can involve coercion or transfer of debts (e.g., owed money exchanged for labour).

The following table (Table 1) provides an overview of recruitment methods and communication channels, providing an overview of their operation. It is important to note that recruitment commissions, although varying by actor, can be highly lucrative; for instance, one criminal group reportedly earned US$1.67 million for trafficking 82 workers to Cambodia via Taiwan Taoyuan International Airport (United Nations Office on Drug and Crime, 2024).

victims within the broader anti–trafficking legal discourse; and 2) it can perpetuate misleading assumptions regarding the socio and technical skills of the victims (e.g., implying they are highly educated or even technologically proficient) – a characterization that is particularly inaccurate for many Chinese survivors (Franceschini et al., 2024) – and may reinforce societal scepticism and institutional bias, leading authorities and the public alike to question the legitimacy of their "victimhood". Public reluctance to recognize individuals trapped in scam compounds as genuine victims is partly rooted in awareness of the psychological suffering and financial harm they inflict on the targets of their scams. Indeed, even when these individuals are deprived of freedom, abused and coerced, doubts persist that they may have known what they were signing up for, or that they might have been complicit in the scam frauds (Franceschini et al., 2025). Criminological research helps contextualize these dynamics through the lens of victim–offender overlap, a theory first developed in the 1950s by criminologists Wolfgang (1957) and von Hentig (1948), which questions the dichotomy between victims and perpetrators by recognizing that individuals can occupy both roles simultaneously (so-called "one-and-the-same" individuals). Originally applied to cases as victim–precipitated homicide, it has been extended to economic crimes like pyramid schemes and online fraud, as well as to intimate–partner violence and even sex trafficking (Fattah, 1991).

In the context of scam compounds, this perspective helps explain how coerced individuals may engage into recruitment or fraudulent activities under duress (either to secure their survival or to meet the imposed quotas), underscoring the complex interplay of coercion, survival strategies and agency, showing how these factors complicate simplistic moral or legal judgments about culpability, a point to which the discussion will return in relation to the potential criminalization of scam cities' survivors.

2.2 Criminal Organization and Role-Based Management

Having examined the broader dynamics of scam cities and their emergence as criminal hubs, it is now necessary to turn to the internal organization of scam compounds. These compounds represent the operational core of transnational cyber-fraud, functioning simultaneously as spaces of confinement, exploitation and industrial-scale criminal production. The scam compounds are structured as highly organized entities, often resembling corporate environments with dedicated departments, managerial hierarchies and specialized roles.

The following section will first reconstruct the structural features of scam compounds – their physical organization, security measures and compartmentalization – and then move to a detailed analysis of the role–based management system that underpins their functioning. This dual perspective highlights how compounds operate both as sites of coercion, akin to spaces of forced labour and as rationalized criminal enterprises where tasks are divided, monitored and enforced with corporate-like precision.

Compounds represent the operational core of the so–called scam cities. They consist of residential and commercial spaces transformed into closed and highly organized criminal hubs, where large–scale cyber–fraud activities are carried out, often in combination with human trafficking and forced labour. Unlike simple clandestine operational centres, compounds are configured as semi–self–sufficient and militarized communities, characterized by tight control over the workforce and a clear separation from the surrounding social fabric (Amnesty International, 2025). The concept of the compound therefore, does not merely designate a "fraud building", but rather a complex infrastructure that integrates logistics, security, labour management and internal economic functions (Global Initiative Against Transnational Organized Crime, 2025; Lazarus et al., 2025). From a physical and spatial perspective, scam compounds do not present a uniform configuration but instead extend along a continuum ranging from fortified and heavily secured structures to residential buildings with an appearance of normality. In the most visible cases, compounds occupy entire gated complexes, often former casinos, resorts, or disused hotels converted into centres for fraudulent activities. In such contexts, security measures are particularly strict and include high perimeter walls, barbed wire, video surveillance systems and armed guards stationed at entry points. These structures resemble private prisons, designed not only to discourage external access but, above all, to restrict the freedom of movement of workers inside, who can leave only with prior authorization (Franceschini et al., 2025). Alongside these openly coercive forms of control, there are also less conspicuous compounds, often located in ordinary condominiums or multi–story buildings which, from the outside, do not display any particularly suspicious features. In such cases, security is enforced not through visible physical barriers but through digital controls and internal surveillance systems, with private guards and restrictions on the movement of occupants. Although lacking the imposing appearance of walled citadels, these structures perform the same function: ensuring the forced containment of the workforce and preserving the operability of criminal activities without attracting excessive external attention (Franceschini et al., 2025; Global Initiative Against Transnational Organized Crime, 2025).

The internal organization follows a functional and compartmentalized logic. On the lower floors are located

logistical services (small supermarkets, canteens, restaurants), designed to minimize contact with the outside and to render the community self-sufficient. The intermediate floors are dedicated to the training of newcomers and to the actual operational activity: large open spaces equipped with rows of computers and telephones from which online frauds are carried out. Operational rooms are often specialized by type of scam or by geographic market: some dedicated to pig butchering, others to impersonating public authorities, still others to fraudulent investments or phishing. The upper floors are reserved for dormitories, where workers live under surveillance, with barred windows and overcrowded spaces (Franceschini et al., 2025; Lazarus et al., 2025).

In addition to offices and dormitories, compounds include spaces dedicated to discipline and control, such as the so-called "black rooms" or "punishment rooms," used to detain and abuse those who attempt to escape or fail to meet imposed targets (Global Initiative Against Transnational Organized Crime, 2025). The presence of these areas reveals the coercive nature of the organization, which combines formalized corporate models with practices typical of illegal detention. Another characteristic feature is the function of a self–sufficient community. Within the compounds one finds clinics, pharmacies, hairdressers, clubs, brothels and even casinos, which are not intended to improve workers' living conditions but rather to entrap them in an internal economy controlled by the organization. Wages, when actually paid, are largely reabsorbed through consumption imposed at inflated prices, fostering a cycle of indebtedness that reinforces the condition of subordination.

The so-called scam compounds must therefore be analysed not only as spaces of confinement and coercion, but also as veritable corporate entities, characterized by an internal structure that reproduces organizational models typical of the private sector. Although not always formally registered, these organizations are often referred to as "online investment companies", a term that reflects both the self–perception and the external representation of such structures (Franceschini et al., 2024; United Nations Office on Drug and Crime, 2025).

The organizational structure of scam cities is articulated along a dual dimension that combines an external level of criminal governance with an internal level of corporate micro–structuring. On the external level, the functioning of the compounds relies on a diversified network of actors performing complementary roles (Asia Foundation, 2025; Global Initiative Against Transnational Organized Crime, 2025). Among these are IT personnel, consisting of technicians and digital operators who, either voluntarily or under coercion, provide central services in cybersecurity, server management and money laundering, often through cryptocurrency transactions. Alongside them operate corrupt officials belonging to police forces, military units and border services, whose role is not only to facilitate the transfer of recruited workers to the compounds but also to guarantee political protection and judicial impunity by neutralizing inspections, controls and potential law enforcement operations. An equally strategic role is played by operations managers, predominantly linked to Chinese–speaking criminal networks but often working in collaboration with local groups or others from Asian countries, who oversee the daily coordination of fraudulent activities and site security (Laungaramsri, 2025). Constantly feeding this ecosystem are recruiters and traffickers, actors operating along transnational chains who, often posing as legitimate job agencies, lure victims with false employment offers and subsequently transfer them into the compounds. Finally, the so–called role shifters – entrepreneurs, politicians and crime bosses – embody the fusion between the legal and illegal spheres: they exploit their economic and political influence to direct investments, shape regulatory processes and manipulate law enforcement agendas, thereby conferring structural stability on the criminal system.

On the internal level, compounds take the form of true simulated corporate organizations, structured into functional departments that reproduce the division of labour typical of enterprises:

—Human resources departments are responsible for recruitment (often forced), contractual and disciplinary management of personnel, while at the same time serving as instruments of social control.

— Operational offices represent the core of the criminal activity: here, the fraud itself takes place, through the creation of fake profiles, direct interaction with victims and the elaboration of psychological manipulation strategies.

— Logistical units, in turn, perform technical tasks essential for productive continuity, such as IT maintenance, formatting of electronic devices, management of communication platforms and so-called phone brushing.

The internal hierarchy is organized with extreme precision: at the top stands the head of department, who supervises the entire operational sector and directs its strategies; immediately below are the core managers, tasked with motivating workers, transmitting fraud technique and monitoring the progress of interactions with defrauded "clients"; next are the team leaders, responsible for training new recruits, maintaining discipline and managing teams; finally, at the base of the pyramid, the

scammers, the material executors of digital fraud, in charge of luring, manipulating and deceiving victims.

This pyramidal model, closely analogous to that of call centres or service companies, is not devoid of incentive mechanisms: commissions, bonuses and performance–based rewards help maintain high productivity, reproducing dynamics typical of formally legitimate enterprises, but within a context of exploitation and coercion that transforms workers into instruments of organized crime.

2.3 Fraud Pedagogy: Training and Schemes Fraud

Having outlined the internal architecture of scam compounds and the central role of managerial and administrative structures in the normalization of coercion, the analysis must now focus on the functional mechanisms through which such structures are translated into operational practices. In this regard, the training of recruits is the key link between systems of internal control and the external implementation of fraudulent schemes. The training process represents a structural and systematic element of the functioning of the compounds, aimed at transforming new recruits into operators fully integrated into the chain of digital fraud. Once recruited – often through deceptive job offers or, in some cases, by means of forced transfers – individuals are subjected to an initial training phase that serves a dual function of coercive socialization and technical instruction.

First, compounds organize actual courses, sometimes presented as language or computer schools, which provide the linguistic and cultural skills necessary to construct credible false identities when interacting with victims, as well as basic digital skills essential for managing online platforms. In parallel, workers are paired with core managers and team leaders in a process of learning by doing: new recruits observe "senior chatters" as they interact with victims, learn techniques of emotional manipulation and gradually progress from simulation to the direct execution of conversations. This training is firmly embedded within the internal division of labour, which distinguishes between those who gather contacts, those who cultivate the relationship with the victim and those who finalize the fraud by requesting money or investments. Alongside relational training, there is also targeted technical instruction: the use of fraudulent financial applications, the management of manipulated cryptocurrency wallets and the deployment of automation tools to maximize efficiency (Asia Foundation, 2025; Global Initiative Against Transnational Organized Crime, 2025; United Nations Office on Drug and Crime, 2025).

Added to this is a disciplinary and coercive dimension: newcomers often undergo a "trial period" during which they receive no pay but are evaluated on the basis of their performance; failure to reach quotas or attempts at resistance result in financial penalties, corporal punishment, or detention in black rooms. What emerges is thus a hybrid model of training, combining corporate strategies of professional instruction with coercive practices typical of forced labour, transforming the compounds into genuine "fraud factories" capable of industrializing human exploitation and maximizing illicit profits on a global scale.

It is precisely through this systematized training process that recruits are progressively directed toward the application of specific fraud schemes, according to a model that replicates the logic of service industries but within a coercive context. Training, in fact, does not constitute an end in itself, but rather a preliminary and necessary phase that functions as a mechanism of "criminal enablement": coerced workers are transformed into specialized executors, capable of carrying out fraudulent practices with an increasing degree of autonomy and sophistication. The result of this training process is the specialization of recruits in different models of digital fraud, which together constitute the true productive architecture of the compounds. The activities carried out within scam compounds are therefore organized through a set of highly diversified and constantly evolving techniques, all of which rely on strategies of social engineering and the use of illicit technological infrastructures (Wang & Zhou, 2022).

To better understand the variety and evolution of these practices, a systematization of the main types of fraud is presented below, categorized according to objectives, tools and operational modalities (Table 2).

2.4 Illicit Monetary Flows

Illicit proceeds derived from scams and online fraud constitute the principal source of income for criminal networks, with substantial revenues generated through the global targeting of victims, via the scam strategies outlined above, paralleled by equally varied mechanisms employed to appropriate victims' funds. The mechanisms through which scam operators access victims' funds are diversified, spanning from the redirection of transfers into mule accounts or shell companies controlled by criminal laundering networks – often under the guise of "legitimate investments"– to the exploitation of the cryptocurrency system (Amerhauser & Thill 2025). In such cases, victims are induced to convert fiat currency into crypto through legitimate exchanges and then connect their digital wallets to fraudulent investment platforms, often embedded within mobile applications or websites, which are engineered to mimic legitimacy. Once victims grant access, the platforms deploy malicious tools –

Table 2: Fraud schemes

Fraud type	Brief Description	Economic Objective
Pig-butchering scam	A combination of romance fraud and investment scam. The victim is groomed over weeks or months and persuaded to invest in platforms secretly controlled by scammers.	Gradual extraction of capital, often reaching hundreds of thousands of USD.
Task scam/Fish–butchering	Victims are recruited with promises of small commissions (e.g., online reviews, traffic boosting), then trapped in tiered "membership" schemes requiring increasingly high deposits.	Lock victims into a cycle of upfront payments and unrecoverable investments.
Impersonation scam	Scammers pose as trusted authorities (police, embassies, customer service) using spoofed numbers and forged documents to extort money.	Direct extortion under threat of legal or reputational consequences.
Crypto Ponzi schemes	Fraudulent investment programs in cryptocurrency promising high returns with little risk, paying 'profits' to earlier investors with funds from newcomers.	Maximize fund collection until the inflow of new victims collapses.
E–commerce scams	Fake stores or listings on legitimate platforms offer counterfeit or non–existent goods; payments are diverted to untraceable channels.	Small profits multiplied by large numbers of victims.
Sextortion/Online extortion	Victims are lured into intimate chats or video calls, which are secretly recorded and later used for blackmail.	Quick payments to prevent dissemination of compromising material.
Phishing & smishing	Fraudulent emails/SMS imitating banks, couriers, or institutions redirect victims to fake websites to steal credentials.	Theft of banking data and direct financial fraud.
Malware/Ransomware	Malicious software infects devices to steal data or lock systems, with ransom demanded (often in crypto).	Extortion via ransom payments or resale of stolen data.
Predatory loan scams	Ads for easy loans lure victims into paying upfront fees or downloading apps that exfiltrate personal data, later used for blackmail.	Profit from deposits and subsequent extortion through stolen data.
Fake kidnapping scams	Victims, often students, are persuaded to stage fake kidnappings (sometimes evolving into real abductions), with videos sent to families to demand ransom.	Extraction of ransom payments ranging from tens to hundreds of thousands of USD.

such as cryptocurrency drainers or fraudulent smart contracts – in order to illicitly extract funds from their wallets, which are then rapidly transferred across multiple accounts and financial institutions, to obscure their trace (Chainalysis, 2024). To this end, gateway companies play a pivotal role, facilitating the execution of transactions within an illicit market where legal rules and protections are absent (Franceschini et al., 2025). By providing this infrastructure, they enable criminal networks to launder sums, exemplified by a Cambodia–based company through which at least US$49 billion in cryptocurrency flowed between 2021 and 2024, much of it linked to risky or illicit counterparties (Elliptic, 2024).

However, it should be noted that payments from scam victims constitute only a portion of the financial movements generated by a scam compound; in the following list, both inflows and outflows are examined to reconstruct the full spectrum of fund flows and to elucidate how the ecosystem sustains itself (Amerhauser & Thill, 2025). Specifically, a "compound economy" generates and circulates money through multiple interconnected channels, which can be summarized in the following categories (Table 3):

Table 3: Compound economy mapping

Category	From/To	Payment mechanism & Notes
Scams and frauds payments	From: Scam victims → To: Criminal groups	Bank transfers, digital wallets and cryptocurrencies; main source of illicit revenue.
Recruitment fees	From: Prospective victims → To: Recruiters / Traffickers	Fees paid to secure "jobs" (travel, facilitation, "tea money"). Payments in cash, digital or hawala; often converted into debt upon arrival.
Scammer (low) compensation	From: Criminal groups → To: Scam workers	Minimal pay, delivered in cash, digital payments, or prepaid cards, sometimes in goods; wages are often withheld or deducted, creating debt bondage.
Ransom Payments	From: Families/Friends → To: Criminal groups	Cash or digital currencies for releasing workers; payments may not guarantee freedom.
Operational expenses: rent	From: Criminal groups → To: Property owners / Businesses	Rent of buildings/floors/rooms for scam operations; payment methods often unknown.
Operational expenses: utilities and services	From: Criminal groups → To: Local utility companies / Service workers	Cash or local digital payments for internet, electricity, water, cooking, and cleaning.
Operational expenses: scam–related IT services	From: Criminal groups → To: online merchants/ companies (Crime–as–a–Service)	Digital or crypto payments; for software, websites, as–a–service tools.
Entertainment (in–house) services	From: Criminal groups operators/scammers → To: Entertainment workers	Workers (often women) provide entertainment, including sexual services, in scam–operated venues; likely paid in cash or online payments; victims often trafficked.
Recruiters & venue managers compensation	From: Criminal groups → To: Recruiters/ Traffickers/ Venue managers	Payments for recruiting victims and managing venues; cash, digital, prepaid cards or crypto; sometimes a percentage of victims' earnings.
(Re–)sale of trafficking victims	From: Compound owners → To: Other compound owners	Payments for transferring or selling victims between compounds; cash, digital or crypto.
Bribes & corruption	From: Criminal groups → To: Officials/Law enforcement agencies	Cash or digital bribes to avoid detection or gain protection.

This mapping of illicit financial flows – spanning revenues from scams, human trafficking and forced labour, as well as payments for bribes and the everyday operations of scam compounds – is crucial to comprehend the functioning of these (both cyber and physical) criminal ecosystems. Professional money laundering service providers play a central role in this process (United Nations Office on Drug and Crime, 2025). By exploiting crypto, online payment systems, mule accounts and fintech platforms, they enable criminal groups to conceal the origin of funds and reintegrate them into the "formal" economy. Although investigative tools such as blockchain analysis and financial monitoring can shed light on parts of these flows, they rarely expose the ultimate beneficiaries (so called "big fish"). This opacity is reinforced by the conversion of proceeds into high–value assets such as real estate, luxury goods, precious metals, offshore accounts or charitable donations, all of which provide a veneer of legitimacy (Amerhauser & Thill 2025). Consequently, a comprehensive 'follow-the-money' approach is not only a practical tool for disrupting illicit flows but also a policy imperative, essential for mitigating the economic and societal harms of cyber scam operations, even if it does not immediately uncover their top–level profiteers. This discussion lays the groundwork for the subsequent examination of measures aimed at preventing, counteracting and supporting efforts to curtail the operations of scam cities.

3 Time-Oriented Frameworks for Countering Scam Cities

The preceding section provided an account of the full "lifecycle" of a scam city, illustrating how individuals are recruited, confined and exploited within these operations. The following section focuses on both immediate/long–term proposals intended to address the phenomenon at different stages of its progression. These are organized according to a temporal framework encompassing three critical phases: 1) prevention, which seeks to mitigate risk and address factors prior to the occurrence of the illicit activities; 2) enforcement, which is directed at ongoing operations to dismantle criminal

networks and ensure perpetrator accountability; and 3) post–release support, which manages the exit of victims from the compounds and the challenges associated with their social reintegration.

3.1 Prevention: Disincentivizing Scam-Base Compounds

Given the discussion thus far, it can be inferred that criminal organisations may find it more advantageous to establish and rely on compound economies rather than contracting independent online fraud "mercenaries" or purchasing hacker-for-hire services. Notably, scam cities offer strategic benefits, including: centralized control and monitoring of coerced workers, economies of scale, reduced operational costs through trafficked labour and even the protection afforded by operating in jurisdictions marked by weak governance or corruption. As this is a rationally chosen criminal business model, effective responses must prioritise prevention in order to make such a choice "less attractive" and harder to implement. To this end, preventive strategies can be conceived as a two–level approach, targeting both "primary" and "secondary" victims.

For primary victims – those who are directly targeted and ultimately defrauded by online scams – prevention should focus on awareness and information campaigns that enhance digital literacy, teach users to recognise common signs of fraud (e.g., promises of unrealistic investment returns or unsolicited requests for financial information) and promote safe online practices to reduce susceptibility to online scams (e.g., verifying the identity of contacts or avoiding suspicious links and downloads). These preventive strategies are crucial, as the communications crafted to exploit primary victims are often deliberately friendly and seemingly innocuous. For instance, Bayu, a 23–year–old Indonesian trafficked to a scam compound in Cambodia, described the messages he was instructed to send to Americans: initial interactions included greetings as: "Good evening, do you have a cat or a dog?" or "Hello, we've met before? and questions like "Do you have any recommendations for a holiday?". These messages, though appearing harmless, were designed to elicit personal data, as WhatsApp contacts, emails and other digital identifiers (Rappler, 2024). Once obtained, this information was used to establish trust and maintain ongoing communication with the victims, gradually manipulating them into disclosing financial details and ultimately persuading them to invest in fraudulent crypto–schemes.

For secondary victims – those who may be trafficked and coerced into participating in scams – prevention can include physical interventions (Franceschini et al., 2025). In Taiwan, authorities have deployed officers at airports to alert travellers about potentially risky job offers in Southeast Asia, aiming to prevent them from unknowingly travelling to high–risk areas. Similarly, the Philippines Bureau of Immigration has regularly issued warnings to citizens considering work in Thailand, Cambodia, Laos or Myanmar, particularly for positions in customer service or other remote online employment. Preventive measures should also emphasize local education about recruitment strategies, early recognition of exploitative job offers (e.g., generic opportunities promising high salaries with little experience required) and awareness of the risks involved in fraudulent employment schemes. An example, drawn from interview–sourced literature, shows a 2020 post on a Facebook group for jobseekers in Cambodia: "Are you looking for work? I have a job for a man or woman between 18 and 30, 6,000 yuan with possible salary raise depending on your performance" (Franceschini et al., 2025), which exemplifies the type of misleading offers that educational interventions could help individuals identify and avoid.

Nonetheless, in both scenarios, enhanced platform regulation and accessible reporting channels could serve as a preventive tool against approaches targeting primary and secondary victims. Indeed, social media, messaging apps and online job boards facilitate the rapid circulation of fraudulent communications, thereby creating conducive conditions for scam-related activities to proliferate. Technically, implementing these measures requires integrating automated checks to confirm the legitimacy of job postings (e.g., cross–referencing company registrations and verified employers), or deploying machine learning models to monitor messaging patterns (e.g., detecting phishing language or repeated suspicious requests) and providing intuitive interfaces for users to report content, with backend systems to process, categorize and escalate reports efficiently. By integrating technical measures within a robust and harmonized regulatory framework, these interventions have the potential to diminish the exposure of both primary and secondary victims, while simultaneously undermining the efficiency of scam compounds, limiting their ability to recruit and exploit individuals through digital channels.

3.2 Enforcement: Repression and Transnational Coordination

Preventive strategies are undoubtedly essential in mitigating the risks that facilitate recruitment and trafficking into scam cities; still, their efficacy proves limited in the absence of robust enforcement mechanisms. Indeed, prevention can only reduce vulnerability ex ante, but once criminal infrastructures are established and operational, the legal order must confront them through coercive instruments

of investigation, prosecution and international cooperation. It is precisely in this second phase that the role of the legal–criminal framework becomes decisive. Against this backdrop, particular attention must be devoted to the 2000 United Nations Convention against Transnational Organized Crime – commonly known as the Palermo Convention – and its supplementary Protocols, which stand as the principal international instruments for addressing the most pervasive manifestations of transnational criminality (United Nations General Assembly, 2000b).

Ratified by more than 190 States, the Convention represents a systemic turning point in the development of international criminal law, as it marks the transition from a model exclusively centred on state sovereignty and the principle of territoriality to a cooperative, multi–level perspective, in which the effectiveness of repressive action decisively depends on coordination among national legal systems. Its innovative scope lies, in particular, in the adoption of a comprehensive approach that not only prescribes obligations of criminalization, but also introduces duties of prevention, instruments of legislative harmonization and, above all, binding mechanisms of judicial cooperation and mutual legal assistance, thereby establishing itself as the cornerstone of the modern system for countering transnational organized crime (Europol, 2023). In particular, the Additional Protocol on Trafficking in Persons to the Palermo Convention provides a definition which, although elaborated in 2000, proves to be still remarkably relevant and capable of encompassing contemporary forms of exploitation connected to scam cities. Art. Article 3 of the Additional Protocol establishes that "*trafficking in persons*" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means such as coercion, deception, fraud, abuse of power or of a position of vulnerability, for the purpose of exploitation (United Nations General Assembly, 2000a). The latter includes, at a minimum, the exploitation of the prostitution of others, forced labour, slavery or practices similar to slavery (Gauci & Magugliani, 2023). Of particular significance is the provision according to which the victim's consent is irrelevant whenever any of the means listed have been employed, as well as the provision that qualifies as trafficking even the mere recruitment or transfer of minors for the purpose of exploitation, regardless of the use of coercive means (United Nations General Assembly, 2000a).

Assessed in light of these criteria, the condition of workers recruited through false promises of employment, transferred via transnational trafficking networks and subsequently compelled, within the compounds, to engage in online fraud activities, fully falls within the legal notion of trafficking as delineated by the Protocol (Asia Foundation, 2025). These individuals are subjected to a coherent sequence of typified acts: from the initial deception to the transfer, culminating in confinement within coercive spaces, followed by exploitation through forced labour. This trajectory faithfully reproduces the concatenation of constituent elements identified in Art. 3. Nor can the possible payment of a salary be deemed relevant to exclude such legal qualification, since as clarified by the European Court of Human Rights (2023): "the remuneration does not annul the status of victim when the work is performed under conditions of coercion, abuse or structural vulnerability". The Court, in fact, emphasized that the systematic deprivation of earnings creates a condition of economic dependency that deprives the victim of the resources necessary for self–emancipation and keeps her in a position of structural vulnerability. From this perspective, "under the Anti–Trafficking Convention's definitions, such consent is irrelevant if any of the 'means' of trafficking have been used" (European Court of Human Rights, 2023).

From this reconstruction it follows that individuals employed within scam compounds cannot be qualified as mere accomplices to fraudulent conduct, but must rather be recognized as victims of trafficking and forced exploitation. This entails the application of the legal corollaries that international law attaches to such status: from protection and assistance at the stage of identification, to the principle of non–punishment for acts committed under coercion, as enshrined both in treaty law and in jurisprudence. It follows that the phenomenon under consideration uniquely combines cybercrime and human trafficking, giving rise to a hybrid form of criminality that poses significant challenges to the current international legal framework. This convergence, though in principle reconcilable with the conventional regime, nonetheless demands a further interpretative and systemic effort: *de iure condendo*, the adoption of an Additional Protocol dedicated to cyber-enabled trafficking schemes appears necessary, in order to clarify and adapt the conventional framework to such phenomena.

For the States Parties – including Myanmar, Thailand, Laos and Cambodia – this translates into stringent obligations of criminalization, victim protection and, above all, transnational cooperation, which is essential to address offences that, by their very nature, transcend jurisdictional boundaries and unfold in liminal spaces beyond effective state control. In this context, Art. 28 of the Convention, which calls upon States to analyse emerging criminal trends and to share common methodologies, assumes particular significance, serving as a bridge between academic observation and international policy–making. The adoption of an Additional Protocol would thus reinforce the Palermo framework, placing it in dialogue with the most recent initiatives in the digital sphere, including

the 2024 UN Convention on Cybercrime. In particular, it would allow for: 1) the introduction of common standards for victim identification and protection, preventing instances of secondary victimization already highlighted by United Nations Office on Drug and Crime (2025); 2) the imposition of enhanced obligations of enhanced cross–border enforcement cooperation in investigations and proceedings relating to transnational online fraud schemes; 3) the establishment of legislative harmonization mechanisms capable of addressing the grey areas generated by the intersection of human exploitation and technological criminality. Although progress at the normative level constitutes an indispensable step, it risks remaining insufficient if not accompanied by an adequate operational architecture that is both stable and transnational. In this direction lies the proposal, advanced in recent policy reports, to establish a Scam Action Task Force (SATF) at the global level, conceived on the model of the Financial Action Task Force (FATF), which has represented a paradigmatic precedent in the fight against money laundering and terrorist financing. The SATF should be structured as a permanent body, placed under the auspices of the United Nations or, alternatively, integrated as a specialized unit within Interpol, thereby combining institutional legitimacy with the capacity for operational coordination with the law enforcement authorities of member States (Sardine & Operation Shamrock, 2025). The proposal would endow the Task Force with binding standard-setting powers, mechanisms of mutual evaluation (peer review) and real–time intelligence-sharing capacities. Its primary mandate would consist in dismantling the criminal infrastructures underlying scam compounds, servers and cryptocurrency flows used for money laundering. At the same time, its mission would not be exhausted in the repressive dimension, but would expressly encompass the liberation, protection and reintegration of victims, thereby outlining an integrated approach in which law enforcement action and the safeguarding of fundamental rights mutually reinforce each other. In this perspective, the SATF is conceived not merely as a technical–operational instrument, but as a mechanism normatively oriented toward the centrality of the victim, placing emancipation and social reintegration at the structural core of the multilateral response.

3.3 Post-Release: Victimhood vs. Criminalization

Thus far, the analysis has focused on the processes through which individuals are recruited and confined within scam walls, as well as the conditions under which they reside there. Equally relevant, however, is to consider the mechanisms through which victims may exit these compounds and the subsequent post–release experiences. Individuals generally have three main options: 1) relatives or friends may attempt to raise the ransom demanded by the operators, although this option is extremely costly and offers no guarantee of release; 2) victims may try to alert authorities, embassies, journalists or other external actors through distress messages, but such attempts are tightly monitored and may even exacerbate their situation; 3) victims may seek assistance from civil society and NGOs, which can provide medical care, psychological support and logistical help for repatriation – often in coordination with survivors or local business networks engaged in rescue efforts (Franceschini et al., 2025).

However, exiting a scam compound rarely marks the conclusion of the obstacles faced by those who were confined within it. While, according to the international conventions recalled in the previous section, the law should extend protection to individuals trafficked and coerced into criminality, this is not always the case for those entrapped in Southeast Asia's scam industry. Indeed, several countries in the region have adopted domestic anti–trafficking legislation inspired by international instruments such as the Palermo Protocol, but with varying degrees of specificity regarding forced criminality. Thailand's Anti–Trafficking in Persons Act of 2008, for instance, enshrines the so-called non-punishment principle, exempting victims from prosecution. Yet, its scope is limited to a narrow set of offences – namely immigration violations, the use of false information or forged documents, prostitution–related offences and illegal employment (Franceschini et al., 2025). This leaves a notable gap with respect to emerging forms of coerced participation in cyber fraud, producing a lack of convergence between being identified as a "victim" of trafficking and being exploited through the perpetration of online scams. As a result, whether coerced individuals are recognised as victims or prosecuted as offenders often depends on the discretion of frontline law enforcement officers and their own interpretation of ambiguous legal categories. A comparable dynamic can be observed, by way of analogy, in the migration context. Notably, cases have emerged in which individuals compelled to steer boats carrying migrants across the Mediterranean are prosecuted as smugglers rather than recognised as coerced actors operating within broader trafficking networks. This reproduces the same paradox: persons subjected to exploitation are classified as offenders, and their victimhood becomes legally and institutionally obscured.

These gaps in legal protection are compounded by practical issues. Survivors are often required to provide "proof of coercion" that directly and causally links their trafficking experience to the criminal acts they performed – an almost insurmountable burden given that job contracts signed under coercion, confiscated communication devices, erased digital traces and subtle forms of punishment (designed to leave no visible marks) undermine the possibility of substantiating their

victim status. In some cases, authorities may even categorise these situations as mere labour disputes (as has happened in Cambodia), while NGOs emphasise their forced–labour dimension (Franceschini et al., 2025). This impasse reveals that the issue is not only legal but also deeply criminological. The difficulty in recognising coerced individuals as legitimate victims recalls the theory of the "ideal victim" (Christie, 1986), in which only certain profiles – such as the weak, innocent or blameless – and behaviours – such as passivity and moral conformity – align with socially accepted notions of 'victimhood. Survivors of scam compounds often fail to meet these expectations, especially when traces of apparent complicity are interpreted as evidence of voluntariness, despite the coercive conditions in which they lived.

The consequences are far-reaching: denial of victim status exacerbates social stigma, hampers reintegration and discourages survivors from coming forward, further contributing to the "dark figure" (or number) of crime in a field where underreporting is already endemic.

4 Conclusion

From a "prognostic" standpoint on the future trajectories of the scam cities phenomenon, the criminological theory of rational choice (Cornish & Clarke, 1986) offers a particularly useful interpretive lens. Building on Beckerian economic analyses of crime (Becker, 1968), this theoretical framework conceives criminal conduct as the outcome of a utilitarian calculus, whereby individuals weigh the relative costs and benefits of illicit opportunities against those of lawful alternatives. In simplified terms, the equation – applicable to the criminal activities within scam compounds – can be structured as follows: a low perception of risk (e.g., detection, arrest and conviction), high expected profits (generated through illicit activities) and relatively low effort required to carry out the offenses (for instance, facilitated by as–a–service models that support scam operations). This perspective underscores the need for responses that are not limited to singular interventions but instead adopt a composite and multi–dimensional approach. Measures can be categorized from three perspectives:

Preventive measures, include: 1) raising digital literacy and awareness campaigns for primary victims (potential scam targets), enabling them to detect early signs of fraud; 2) targeted interventions for secondary victims (potentially trafficked workers), such as airport checks, consular alerts, education on deceptive recruitment, and tighter regulation of online job platforms.

Enforcement strategies, focus on: 1) strengthening international legal instruments, by interpreting scam compounds under the Palermo Protocol (United Nations General Assembly, 2000b) framework and, *de iure condendo*, exploring a dedicated protocol on cyber–enabled trafficking; 2) enhancing transnational coordination through specialized task forces (e.g., a Scam Action Task Force modelled on FATF), with real-time intelligence–sharing and capacities to disrupt illicit financial flows and infrastructures.

Ex post measures, designed to: 1) ensure recognition of coerced workers as victims of human trafficking rather than accomplices, through the application of the non–punishment principle; 2) support survivors' reintegration with medical, psychological and legal assistance, while addressing stigma and barriers created by narrow or ambiguous "victimhood" definitions.

Moreover, this perspective highlights the essential role of research in informing both policy and operational measures. Specifically, a mixed–methods approach combining qualitative fieldwork, victim and practitioner interviews, along with quantitative analysis of financial flows and operational dynamics would be valuable in deepening understanding and enabling the development of context–sensitive interventions. In this way, academic research can directly contribute to more effective strategies to mitigate the harms of scam cities and anticipate their future evolution.

References

1. Abraham, I., & van Schendel, W. (2005). Introduction: The making of illicitness. In W. van Schendel, & I. Abraham (Eds.), *Illicit Flows and Criminal Things: States, Borders, and the Other Side of Globalization* (pp. 1–37). Indiana University Press.
2. Amerhauser, K., & Thill, A. (2025). *The business of exploitation: The economics of cyber scam operations in Southeast Asia.* Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/cyber-scam-operations-southeast-asia/
3. Amnesty International. (2025). "*I was someone else's property*": *Slavery, human trafficking and torture in Cambodia's scamming compounds*. https://www.amnesty.org/en/wp-content/uploads/2025/06/ASA2394472025ENGLISH.pdf
4. Asia Foundation. (2025). *Illicit economies and informal governance: How borderland infrastructure in Myanmar enables a scam-based economy*. Asia Foundation.
5. Banks, J. (2016). *Online gambling and crime: Causes, controls and controversies.* Routledge.
6. Becker, G. S. (1968). *Crime and punishment: An economic approach. Journal of Political Economy, 76*(2), 169–217.
7. Chainalysis. (2024). *Money laundering and cryptocurrency: Trends and new techniques for detection and investigation.* Chainalysis.

8. Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy: Reorienting the justice system* (pp. 17–30). Macmillan.
9. Cornish, D. B., & Clarke, R. V. (Eds.). (2017). *The reasoning criminal: Rational choice perspectives on offending.* Taylor & Francis.
10. Elliptic. (2024). *Huione guarantee: The multi-billion dollar marketplace used by online scammers*. https://www.elliptic.co/blog/cyber-scam-marketplace
11. European Court of Human Rights. (2023). Case of Krauchunova v. Bulgaria, Application no. 18269/18. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-229129%22]}
12. Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. https://www.europol.europa.eu/iocta-report
13. Fattah, E. A. (1991). The victimization of women: A criminological perspective. *Canadian Journal of Criminology, 33*(1), 1–24.
14. Franceschini, I., Li, L., & Bo, M. (2023). Compound capitalism: A political economy of Southeast Asia's online scam operations. *Critical Asian Studies, 55*(4), 575–603.
15. Franceschini, I., Li, L., & Bo, M. (2025). *Scam: Inside Southeast Asia's cybercrime compounds*. Verso Books.
16. Franceschini, I., Li, L., Hu, Y., & Bo, M. (2024). A new type of victim? Profiling survivors of modern slavery in the online scam industry in Southeast Asia. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-024-09552-2
17. Gauci, J.-P., & Magugliani, N. (2023). *Human trafficking and the rights of trafficked persons: An exploratory analysis on the application of the non-punishment principle.* International Bar Association Legal Policy & Research Unit & British Institute of International & Comparative Law.
18. Giordana, E., & Morello, M. (2025). Asia criminale: I nuovi triangoli d'oro tra scam citygoli d'oro tra scam city, armi, droga, pietre preziose ed esseri umani [Criminal Asia: The new golden triangles of scam cities, weapons, drugs, gemstones, and humans]. Baldini e Castoldi.
19. Global Initiative Against Transnational Organized Crime. (2025). *Inside the scam compounds: Cyber fraud operations in Southeast Asia*. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia
20. Gore, A., Kennedy, L., Southern, N. P., & van Uhm, D. (2022). *Asian roulette: criminogenic casinos and illicit trade in environmental commodities in South East Asia*. https://globalinitiative.net/analysis/casino-crime-south-east-asia/
21. Hall, T., Sanders, B., Bah, M., King, O., & Wigley, E. (2021). Economic geographies of the illegal: The multiscalar production of cybercrime. *Trends in Organized Crime*, *24*(2), 282–307.
22. Humanity Research Consultancy. (2024). *Uncovering the spread of human trafficking for online fraud into Laos and Dubai.* https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/66a9db2e56d3b112ae6eff39_USAID-Asia-CTIP-Laos-Dubai-Investigation.pdf
23. Laungaramsri, P. (2025). Dark zomia: Myanmar frontier and the Chinese enclosure. *Journal of Borderlands Studies*, 1–16. https://doi.org/10.1080/08865655.2025.2469854
24. Lazarus, S., Chiang, M., & Button, M. (2025). Assessing human trafficking and cybercrime intersections through survivor narratives. *Deviant Behavior*, 1–18. https://doi.org/10.1080/01639625.2025.2470402
25. Rappler. (2024). *Trick messages for WhatsApp - Bayu's experience in a scam compound.* https://www.rappler.com/newsbreak/investigative/fake-profiles-real-victims-cambodian-compound-targeting-americans/
26. Sardine & Operation Shamrock. (2025). *Ending the scamdemic: The case for a global Scam Action Task Force (SATF)*. Sardine.AI.
27. United Nations General Assembly. (2000a). *Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime.* https://www.ohchr.org/sites/default/files/ProtocolonTrafficking.pdf
28. United Nations General Assembly. (2000b). *United Nations Convention against Transnational Organized Crime and the Protocols thereto.* https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html
29. United Nations Human Rights Office of the High Commissioner. (2023). *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response.* OHCHR Bangkok Office. https://bangkok.ohchr.org/news/2022/online-scam-operations-and-trafficking-forced-criminality-southeast-asia
30. United Nations Office on Drug and Crime. (2024). *Casinos, money laundering, underground banking and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat.* https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf
31. United Nations Office on Drug and Crime. (2025). *Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia.* United Nations. https://doi.org/10.18356/9789211542622
32. USIP Senior Study Group on Transnational Organized Crime in Southeast Asia. (2024). *Transnational crime in Southeast Asia: A growing threat to global peace and security.* https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security
33. von Hentig, H. (1948). *The criminal and his victim: Studies in the sociobiology of crime.* Yale University Press.
34. Wang, F., & Zhou, X. (2022). Persuasive Schemes for financial exploitation in online romance scam: an anatomy on Sha Zhu Pan (杀猪盘) in China. *Victims & Offenders*, *18*(5), 915–942.
35. Wolfgang, M. F. (1957). Victim precipitated criminal homicide. *Journal of Criminal Law and Criminology*, *48*(1), 1–11.

Prevarantska mesta: kriminalitetna središča v transnacionalnih omrežjih kibernetske kriminalitete

Sara Lilli, doktorska študentka, Šola za napredne študije Sant'Anna (Pisa) in Šola za napredne študije IMT (Lucca), Italija. ORCID: 0009-0000-2796-3067. E-pošta: sara.lilli@imtlucca.it

Maria Vittoria Zucca, doktorska študentka, Šola za napredne študije Sant'Anna (Pisa) in Šola za napredne študije IMT (Lucca), Italija. ORCID: 0009-0004-0049-9611. E-pošta: mariavittoria.zucca@imtlucca.it

Študija se osredotoča na pojav tako imenovanih »prevarantskih mest«: urbanih ali polurbanih središč, ki so predvsem v jugovzhodni Aziji, kjer kriminalne mreže orkestrirajo obsežne kibernetske goljufije z izkoriščanjem žrtev trgovine z ljudmi, podvrženih prisilnemu delu. Te skupine, ki so pogosto prikrite kot klicni centri ali igralnice, predstavljajo konvergenco kibernetske kriminalitete, trgovine z ljudmi in nadnacionalne organizirane kriminalitete. Kljub vse večji pozornosti novinarjev ostaja ta tema v pravni in kriminološki literaturi premalo raziskana. Študija se razvija vzdolž dveh glavnih osi. Prva preučuje »življenjski cikel« prevarantskih skupin, s poudarkom na: 1) zavajajočih strategijah novačenja; 2) organizacijskih strukturah; 3) uporabljenih goljufivih shemah; in 4) nezakonitih finančnih tokovih. Druga ponuja odgovore v časovnem spektru: 1) preprečevanje, namenjeno zmanjševanju kriminalnih tveganj in krepitvi ozaveščenosti; 2) izvrševanje, usmerjeno v prepoznavanje protiukrepov in s tem povezanih pravnih vrzeli; in 3) podpora po izpustitvi, ki obravnava ponovno vključitev preživelih in njihovo pravno priznanje. Z obravnavo teh razsežnosti želi študija prispevati h globalnim razpravam o prevarantskih spojinah, poglobiti akademsko razumevanje pojava in zagotoviti vpoglede za oblikovanje politik, pravnih okvirov in praktičnih posegov.

Ključne besede: prevarantska mesta, digitalno suženjstvo, mednarodna organizirana kriminaliteta, trgovina z ljudmi, kibernetska kriminaliteta

UDK: 343.341