Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Documented Presence and Process Location of Generative Artificial Intelligence in Industrial Scam Compounds and the Limits of the Transformation Claim

Hamza Khan

hamza.khan@slsh.edu.in

Symbiosis International University

Systematic Review

Keywords: organised crime, generative artificial intelligence, crime scripts, scam compounds, Southeast Asia, cyber-enabled fraud

Posted Date: November 11th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10915629/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

Peer-reviewed research on Southeast Asian industrial scam compounds documents hierarchical, coercive organisation and the presence of generative models, synthetic media and related tools in the operational repertoire. It does not, however, isolate those tools as the measured cause of labour change, success rates or organisational form. This article, therefore, asks a more limited set of questions. First, what does the published record establish about the organisation of compound-based cyber-fraud? Second, where in the crime-commission process are generative and synthetic-media tools located, and at what level of documentation? Third, what remains unshown about transformation? The study is a structured qualitative synthesis of recent peer-reviewed work on compounds, trafficking for forced criminality, cybercrime organisation and generative fraud, supplemented by a bounded strand of official assessments and investigative process sources coded only for the described process, role or tool. Official estimates are reported as official estimates. A composite script table locates documented insertion points without treating presence as effect. Three claims are kept separate: compound organisation is strongly evidenced; generative and synthetic tools are moderately evidenced as repertoire items; AI as a cause of labour, success or form change is not shown. Agentic, multi-step orchestration is distinguished from content generation and is treated as thinly evidenced in the peer-reviewed set. The distinctive contribution is an open adjudication problem: the compound-level measures that would decide between an incremental-tool reading and a reorganisation reading.

1. Introduction

Industrial-scale cyber-fraud compounds in mainland Southeast Asia are now a documented organisational form. Peer-reviewed studies describe walled facilities hosting multiple companies, trafficking into forced criminality, hierarchical labour, and multi-actor facilitation by syndicates, brokers and political or economic elites (Franceschini et al., 2023; Franceschini et al., 2024; Lazarus et al., 2026). The same literature, together with official regional assessments, records the presence of generative models, deepfakes and cryptocurrencies in this environment (Akartuna & Manning, 2026; UNODC, 2026; Lin, 2025; Visconti, 2026; Tiwari et al., 2026). Those two facts are often joined into a stronger claim: that generative and agentic artificial intelligence is a force multiplier that restructures organised crime. That stronger claim is a hypothesis. It is not a finding this article can defend from the evidence it reviews.

The mismatch matters. Systematic reviews of generative AI and financial crime show a sharp rise in scholarly attention after 2022 and a growing focus on automated offending alongside older social-engineering forms (Tiwari et al., 2026). Incident-based work records an increase in AI- and deepfake-enabled fraud cases after public generative tools became widely available (Zhang, 2026). Compound studies report that operations embrace artificial intelligence and deepfakes (Akartuna & Manning, 2026). None of these sources supplies compound-level measures of tasks per operator, languages per operator, time-to-trust, or the share of conversations that are model-drafted. Without those measures, presence and co-location can be stated. Produced, reduced, enabled and shifted cannot.

The empirical domain of this article is compound-based cyber-fraud in mainland Southeast Asia, with limited notes on displacement and export of the model. Victim geography and worker recruitment are transnational. That is not the same as a mapped multi-region organisational form. Non-SEA comparison cases are noted only where official or investigative sources describe similar compound or service arrangements; they are not treated as a second sample.

Three research questions follow. RQ1: What does the peer-reviewed record establish about the internal organisation of industrial scam compounds? RQ2: Where in the crime-commission process are generative models and synthetic-media tools documented, and how should content generation be distinguished from thinly evidenced agent-like orchestration? RQ3: What implications for scale, reach and resilience can be stated without attributing those outcomes to AI as cause?

The contribution is threefold and deliberately limited. The article offers an organisational description of compounds grounded in peer-reviewed work. It locates generative and synthetic tools in process stages using a composite script table that marks cells as documented, inferred or unknown. It reports a negative result on measured transformation and specifies the compound-level evidence that would be required to decide between an incremental-tool reading and a reorganisation reading.

2. Literature and conceptual frame

Organised crime is treated here as an organised activity rather than as a single organisational type. Relational approaches map cooperation as an empirical structure (Campana & Varese, 2020; Campana & Antonopoulos, 2024). Enterprise perspectives emphasise specialisation and market adaptation. Governance perspectives distinguish groups that regulate territories from those that trade in illicit markets (Campana & Varese, 2018). Adaptability is common across these traditions: groups reorganise roles and absorb tools

when opportunity structures change (Campana, 2020; Campana & Meneghini, 2024). New tools therefore need not produce one organisational outcome.

Digital adaptation is not new. Cybercrime-as-a-service commoditises capabilities for less skilled buyers (Hyslip, 2020). Dutch financial cybercrime networks display division of labour and duration, often resembling teams or formal organisations rather than loners (Leukfeldt & Holt, 2020). Related work cautions against equating all cyber offending with classic organised crime while still showing that financial cybercrime can be socially organised (Leukfeldt et al., 2017). That baseline matters. Specialisation and modular supply predate generative models.

Compound-based fraud is a distinct organisational niche. Franceschini, Li and Bo (2023) describe the shift from smaller sites into larger walled compounds and frame the arrangement as compound capitalism: enclosed labour, space and profit extraction sustained by operators, brokers and elites. Franceschini et al. (2024) profile survivors and document deceptive recruitment. Lazarus et al. (2026) synthesise fifty publications from 2020 to 2025 and report hierarchical divisions of labour, coercion and liminal victim-offender roles. Akartuna and Manning (2026) map a multi-actor Myanmar ecosystem of syndicates, armed groups, officials and special economic zones, and note resilience and displacement under enforcement pressure.

Crime script analysis remains the process lens (Dehghanniri & Borrion, 2021; Alonso Berbotto & Chainey, 2022). Scripts specify sequential scenes with actions, roles, tools, settings and dependencies. They do not, by themselves, measure causal effects of a tool. Subsequent applications to organised and complex crimes show that scripts can be populated from open and secondary sources (Matthijsse et al., 2023; Sun et al., 2026). That is the use made here.

Two organisational patterns should not be collapsed. Modular cyber service markets and factory-like compounds can both accommodate generative tools. Compatibility is not dual transformation. The working frame is therefore co-location, not production: tools appear in named stages; organisation is described independently; outcomes of scale and resilience are reported as industry-level findings unless a source isolates AI as cause.

3. Method

3.1 Design

The design is a structured qualitative synthesis, not an original coding of a closed official corpus that is then left unused. A reporting checklist, adapted source-flow, search note and claim-coding rules are provided as Supplementary Files S1–S4. Strand A is peer-reviewed research on compounds, trafficking for forced criminality, cybercrime organisation, crime scripts and generative or synthetic-media fraud, published mainly between 2018 and 2026 in criminology and related journals. Strand B is a bounded set of official assessments and investigative process sources used only to populate script cells that the academic literature leaves empty. Strand B is not treated as peer review. Passages are retained only when they describe a process, role, tool or organisational arrangement. General threat judgements are excluded (Campana & Varese, 2020).

3.2 Sources

Strand A centres on Franceschini et al. (2023, 2024), Lazarus et al. (2026), Akartuna and Manning (2026), Leukfeldt and Holt (2020), Lin (2025), Visconti (2026), Tiwari et al. (2026), Zhang (2026), and crime-script methodological papers (Dehghanniri & Borrion, 2021; Alonso Berbotto & Chainey, 2022). Strand B comprises UNODC's Transnational Organised Crime Threat Assessment for Southeast Asia 2026 (UNODC, 2026), earlier UNODC technical briefs on casinos, cyber-fraud and forced criminality (UNODC, 2023, 2024), OHCHR (2023) on online scam operations and trafficking for forced criminality, and, where they describe process rather than headline threat, Europol's Internet Organised Crime Threat Assessment and the United Kingdom National Crime Agency's National Strategic Assessment for 2026 (Europol, 2026; National Crime Agency, 2026). Investigative process sources, including platform disruption reporting, are used only as corroboration of tool presence and are never the sole support for an organisational claim.

Loss figures are attributed to their issuers. UNODC (2026) estimates combined annual losses from scam offences across East Asia, South-East Asia, Australia and New Zealand at between USD 88.3 billion and USD 114.1 billion for 2025. Akartuna and Manning (2026) report compound-linked global losses in the order of tens of billions of United States dollars. These bands are not reconciled into a single original estimate.

3.3 Inclusion and unit of analysis

The unit of analysis is the fraud process organised by a compound or closely related network in mainland Southeast Asia. Inclusion requires (a) structured group activity over time for material gain (Campana & Varese, 2018), (b) compound or industrial scam organisation, and (c) sufficient process detail to locate at least three script scenes. Generative or synthetic-media tools are coded when named. Cases that describe generic cybercrime without a compound organisation are excluded from the organisational claim set. Diffusion notes (relocation beyond Myanmar and Laos; service-ecosystem language) are labelled as official or investigative observations, not as a second systematic sample. An inclusion log is presented in Table A1 (Appendix A).

3.4 Procedure

Sources were read for three separable claims: compound organisation; tool presence and process location; and any measured link from tools to labour, success or form. A composite script was then built with columns for scene, actions reported, roles, tools, setting, dependencies, possible intervention points, and evidential status (documented in peer-reviewed work; documented only in official or investigative sources; inferred; unknown). Intervention points are dependencies named in sources, not evaluated disruption effects. Dual-source support is required for any organisational sentence that carries a main finding. Uncertainty is retained.

3.5 What this design cannot do

It cannot estimate prevalence of tool use across compounds, attribute a causal effect to AI, or generalise to all organised crime. Official sources are biased toward detected groups. Closed sites are not observed. Technical detail dated 2026 may already be incomplete. No compound-level task-allocation dataset is available in the peer-reviewed set.

4. Findings

Findings are organised as three claims that the earlier draft blended. Claim 1 is strong. Claim 2 is moderate. Claim 3 is not shown.

4.1 Claim 1. Organisation of compounds (strong evidence)

Peer-reviewed studies agree on the organisational form. Operations moved from smaller apartments, villas and hotel rooms into larger walled compounds hosting multiple companies (Franceschini et al., 2023, 2024). Labour is supplied in substantial part through deception and trafficking; workers are held and compelled to perform fraud under coercive discipline (Franceschini et al., 2023, 2024; Lazarus et al., 2026). Cross-study patterns include hierarchical divisions of labour and liminal victim-offender roles (Lazarus et al., 2026). Franceschini et al. (2024) show that Chinese and other survivors often resemble familiar trafficking profiles rather than a wholly new victim type. Wider ecosystems include operators, brokers, syndicates, armed groups, special economic zones and elite facilitation (Franceschini et al., 2023; Akartuna & Manning, 2026). Financially motivated cyber networks outside this region already display division of labour and duration (Leukfeldt & Holt, 2020). That comparison supports reading compounds as organised enterprise. It does not measure how generative tools redistribute tasks inside them.

Official assessments describe a related service-ecosystem pattern: specialised functions for fraud, recruitment, settlement and infrastructure offered across a shared illicit economy (UNODC, 2026). That language is closer to a modular-service hypothesis than anything isolated in the peer-reviewed compound ethnography. It remains an official characterisation, not a peer-reviewed measurement of modularisation caused by AI.

4.2 Claim 2. Presence and process location of generative and synthetic tools (moderate evidence)

Akartuna and Manning (2026) state that compound operations continue to embrace artificial intelligence, deepfakes and cryptocurrencies. Lin (2025) examines deepfake audio and video in organised fraud, including impersonation and identity-related cases. Visconti (2026) reviews generative models and automation in industrialised deception. Tiwari et al. (2026) find a growing scholarly concentration on automated financial crime distinct from older human-centric social engineering. Zhang (2026) reports a rise in documented AI- and deepfake-enabled fraud incidents after 2022. UNODC (2026) records official concern with generative AI, deepfakes and more automated fraud in the regional ecosystem.

These sources support presence and co-location. They do not support a count of compounds that use the tools, nor a measured change in operator workload. Investigative and platform-disruption reporting describes software that drafts replies across languages, maintains personas and monitors operators. Under the dual-source rule those descriptions may fill script cells marked official or investigative. They do not upgrade presence into proven labour substitution.

4.3 Distinguishing generative functions from agentic orchestration

Three functions are separated here. (a) Content generation: model-drafted text, translated copy and synthetic images or audio. This is the best evidenced layer (Lin, 2025; Visconti, 2026; Tiwari et al., 2026; Akartuna & Manning, 2026). (b) Real-time translation and persona maintenance: tools that help an operator sustain contact in a language the operator does not command. Official and investigative sources describe this more often than peer-reviewed compound studies. (c) Agent-like orchestration: multi-step plan, tool use, loop and handoff with limited human steering. Function (c) is thinly evidenced in the peer-reviewed compound set. The title of earlier drafts paired generative and agentic AI as if they were equally documented. They are not. This article restricts the object of study to generative models and synthetic media, and treats agentic orchestration as an open empirical question.

4.4 A composite script: location without effect

Table 1 is a composite script for compound-based romance-to-investment and related high-volume fraud as those processes appear in the reviewed sources. It is not a claim that every compound follows one sequence. Cells marked inferred are not findings. Compression of stages is not claimed.

Table 1
Composite process script for compound-based cyber-fraud (location of tools, not measured effects)

Scene	Actions reported	Roles	Tools (incl. AI type)	Setting	Dependencies	Possible intervention point	Status
Preparation	Compound set-up; deceptive job recruitment; confinement of workers	Operators, brokers, managers, trafficked workers	Digital infrastructure; accounts; generative tools among named technologies	Walled compounds; SEZs; limited-governance zones	Premises, coerced labour, local facilitation	Recruitment pipelines; compound hosting; facilitation	Documented in PR: Franceschini et al. 2023, 2024; Lazarus et al. 2026. AI named: Akartuna & Manning 2026
Targeting	Identification of potential victims; initial contact at volume	Floor operators under quota; targeting or data functions where described	Messaging platforms; possible model-drafted openers and translation	Online platforms; operator rooms inside compounds	Access to accounts and lists; language capacity or translation tools	Platform abuse signals; account farms	Process documented in PR. Tool use in this scene: moderate / official-investigative more specific than PR
Engagement	Sustained contact; romance or investment narrative; identity proof when demanded	Operators; supervisors; technical facilitators	Generative text; translation; deepfake or voice cloning where named	Compound work floor; remote platforms	Time on task; coercive quotas; synthetic-media tools if used	Detection of synthetic media; victim reporting channels	Fraud types documented (Akartuna & Manning 2026). Deepfakes in organised fraud (Lin 2025). No PR measure of conversations per operator
Extraction	Movement of funds into controlled channels	Payment and platform specialists; operators at handover	Fraudulent investment interfaces; cryptocurrency among named rails	Online payment rails; compound-linked settlement services	Payment infrastructure; victim compliance after engagement	Payment-rail disruption; asset recovery	Documented at industry level (Akartuna & Manning 2026; UNODC 2026). AI not isolated as cause of extraction success
Concealment and continuity	Layering of proceeds; relocation; replacement of staff or tools	Laundering services; elite or armed-group protection; managers	Cryptocurrency and service infrastructure; tool substitution possible	Multi-actor ecosystems across borders	Facilitation; alternative sites; replaceable labour and tools	Cross-border financial investigation; hosting and protection nodes	Resilience and displacement documented (Akartuna & Manning 2026; UNODC 2026). Not shown as an AI effect

Note. PR = peer-reviewed. Intervention points are dependencies named in sources, not tested effects. A pig-butchering variant and a shorter investment-funnel variant share preparation, extraction and concealment; they differ mainly in the length and emotional framing of engagement. Sources do not support separate measured scripts for each variant.

Table A1
Source log of included and excluded materials, by type, jurisdiction or focus, claim informed, and inclusion status.

Source	Type	Jurisdiction/focus	Informs	Included
Franceschini et al. (2023).	Peer-reviewed	Cambodia, Myanmar, Laos	Compound organisation; facilitation	Yes - Claim 1
Franceschini et al. (2024).	Peer-reviewed	SEA compounds; Chinese and other survivors	Recruitment; labour; victim profiles	Yes - Claim 1
Lazarus et al. (2026).	Peer-reviewed meta-synthesis	SEA 2020–2025	Hierarchy; coercion; victim-offender roles	Yes - Claim 1
Akartuna & Manning (2026).	Peer-reviewed	Myanmar ecosystem	Multi-actor network; tool repertoire; resilience	Yes - Claims 1–2; scale as cited estimate
Leukfeldt & Holt (2020).	Peer-reviewed	Netherlands cyber networks	Division of labour baseline	Yes - comparison only
Lin (2025)	Peer-reviewed	Organised fraud cases	Deepfakes as repertoire	Yes - Claim 2
Visconti (2026)	Peer-reviewed review	AI and deception	Generative deception literature	Yes - Claim 2; not causal proof
Tiwari et al. (2026).	Peer-reviewed review	GenAI and financial crime	Field growth after 2022	Yes - Claim 2 context
Zhang (2026)	Peer-reviewed incident analysis	Global AI/deepfake fraud cases	Post-2022 case rise	Yes - Claim 2 context
Dehghanniri & Borrion (2021); Alonso Berbotto & Chainey (2022)	Peer-reviewed method	Script method	Script structure	Yes - method
UNODC (2023, 2024, 2026)	Official assessment	SEA / Asia-Pacific	Ecosystem language; 2025 loss band; recruitment geography	Yes - Strand B; official estimates only
OHCHR (2023)	Official	SEA forced criminality	Forced criminality estimates	Yes - Strand B
Europol (2026); NCA (2026)	Official	EU / UK	Process language where present	Yes - Strand B, process only
Generic cybercrime without compound organisation	-	-	-	Excluded from Claim 1 sample
Single-source press on named software stacks	Investigative	Variable	Script cells only	Corroboration; not sole support
Appendix B. What is not shown				
Not shown: tasks per operator before and after tool adoption; languages per operator; time-to-trust; share of model-drafted conversations; substitution of fluent trafficked labour attributable to AI; agentic multi-step workflows inside compounds; a causal effect of AI on success rates; a demonstrated shift from labour-intensive to technology-intensive organisation. Shown: compound organisation; tool presence in the repertoire; process location at scene level; official loss bands; resilience and displacement as industry and network findings.				

4.5 Claim 3. Scale, reach, resilience - and what is not shown

Industry-level scale is reported by issuers, not calculated here. Akartuna and Manning (2026) place compound-linked losses in the tens of billions of United States dollars annually. UNODC (2026) estimates scam losses across a wider Asia-Pacific victim geography at USD 88.3 billion to USD 114.1 billion for 2025. These figures are different constructs. They should not be merged. Reach appears as multi-country victimisation and as recruitment of workers from many nationalities; UNODC (2026) reports people from at least 80 countries and territories identified in regional compounds. Resilience and displacement are documented in network analysis of Myanmar and in official accounts of relocation under pressure (Akartuna & Manning, 2026; UNODC, 2026). Poly-criminal linkage - trafficking for forced criminality inside the same systems that run fraud - is a peer-reviewed organisational finding (Franceschini et al., 2023, 2024; Lazarus et al., 2026).

What is not shown is the causal clause that earlier drafts placed in the abstract. The record does not measure reduced labour requirements, simultaneous multi-language targeting as a counted capacity gain, professionalisation of social engineering as an outcome metric, or a shift toward modular service structures caused by AI. Forced labour persists (Franceschini et al., 2024; Lazarus et al., 2026). Continuity is explained in the literature by compounds, coercion, facilitation and payment infrastructure as well as by technology (Franceschini et al., 2023; Akartuna & Manning, 2026).

5. Discussion

Read against the working frame, the first link - tools appearing in the repertoire and in named process stages - is the only link that the evidence can carry. Organisational adaptation is visible in the compound literature without being reducible to AI (Lazarus et al., 2026; Franceschini et al., 2023). Scale and resilience are industry-level facts with official and peer-reviewed sponsors; they are not isolated AI effects.

Theoretically, generative tools are compatible with both modular cyber service markets (Hyslip, 2020; Leukfeldt & Holt, 2020) and with factory-like compounds (Franceschini et al., 2023; Lazarus et al., 2026). That dual fit is a compatibility argument. It is not a demonstrated dual transformation. Relational perspectives already treat organisation as something to be mapped rather than assumed (Campana & Varese, 2020). The relevant question remains how existing forms absorb tools, not whether AI creates organised crime.

Two readings stay open. An incremental tool reading treats generative systems as additions to compounds, trafficking, facilitation and payment infrastructure that already produce industrial scale (Franceschini et al., 2023; Lazarus et al., 2026). A reorganisation reading treats them as a force that reallocates labour and multiplies capacity (Visconti, 2026; Lin, 2025). Presence data cannot decide between them.

5.1 What would decide the question

The distinctive next step is not another recap. It is an adjudication problem. Compound-level measures that would decide between the two readings include: tasks per operator with and without model assistance; languages handled per operator; time from first contact to fund movement; substitution of fluent trafficked labour after tool adoption; and the share of conversations that are model-drafted rather than human-authored. Until those measures exist, AI is a documented capability inside an already organised industry.

5.2 Implications that do not require AI as driver

Practical implications follow from compound organisation and from tool presence where it is documented. They do not require script compression or AI primacy. Recruitment pipelines and compound hosting remain central dependencies (Franceschini et al., 2023, 2024; Lazarus et al., 2026). Coerced workers are trafficking victims as well as persons compelled to offend (Franceschini et al., 2024). Cooperation that stops at national borders is poorly matched to worker origins, victim geography and displacement (Akartuna & Manning, 2026; UNODC, 2026). Sharing signals on synthetic identity and model-assisted contact is consistent with documented tool presence (Lin, 2025; Visconti, 2026). Displacement after single-point pressure is already reported (Akartuna & Manning, 2026). None of these points treats generative AI as the engine of the industry.

6. Limitations

There is no compound-level task-allocation dataset in the peer-reviewed set. Official sources over-represent detected groups and under-represent groups that have not come to notice. Closed sites cannot be observed. Technical descriptions from 2026 age quickly. The sample is mainland-Southeast-Asian compounds; transnational in the title of earlier drafts overstated mapped multi-region organisation. Strand B official and investigative sources fill process cells but are not peer review. Several widely circulated 2026 academic items were checked for bibliographic completeness; items that cannot be cited with a stable outlet and DOI are not used as load-bearing evidence. The analysis is a structured synthesis plus a composite script, not a primary observation study.

7. Conclusion

Industrial scam compounds are hierarchical, coercive and multi-actor. Generative models and synthetic media belong in their technological repertoire and can be located in preparation, targeting and engagement without converting location into effect. Official estimates place regional scam losses in a high tens-of-billions to low hundreds-of-billions band for 2025, depending on the construct used. Resilience and displacement are documented. What is not shown is the measured transformation of labour, success or form by

AI. Agentic orchestration is thinner still. The safer claim is the presence within the organised industry. The useful next claim is a list of compound-level measures that would allow the incremental-tool reading and the reorganisation reading to be tested rather than restated.

Declarations

Ethics approval and consent to participate

This article does not involve studies with human participants or animals that would require formal ethical approval. Not applicable, no human participants were involved, and no informed consent was required.

Consent for publication

The author has reviewed the final manuscript and consents to its publication.

Competing interests

The author declares no competing interests.

Funding

No funding was received for this research.

Author Contribution

Hamza Khan conceived the study; designed the structured qualitative synthesis; identified, included and coded the sources; constructed the composite process script; wrote the manuscript; and approved the final version.Credit: Conceptualisation, Methodology, Investigation, Formal analysis, Writing – original draft, Writing – review and editing - H.K.

Data Availability

This article is a structured qualitative synthesis of published sources. No primary, author-generated datasets were produced. All sources that inform the three claims are listed in the reference list and in the source log (Appendix A). Materials that allow editors and referees to verify the method - the ENTREQ-aligned reporting checklist, the adapted source-flow diagram, the search approach and inclusion log, and the claim-coding / script-extraction fields - are supplied as Supplementary Files S1–S4 with this submission. Official assessments used only to populate process-script cells remain the property of their issuing organisations and are cited rather than reproduced. No individual-level or otherwise restricted data were collected.

References

1. Akartuna EA, Manning MG (2026) An artificial intelligence-driven temporal network analysis of Myanmar's cyber scam ecosystem. Asian J Criminol 21(1). Article 10. https://doi.org/10.1007/s11417-025-09474-0
2. Akartuna EA, Yeung FSW, Manning M, Bish A (2025) Shifting routines and the industrialisation of scams: The impact of COVID-19 on deception crimes in Hong Kong. *Trends in Organized Crime*. Advance online publication. https://doi.org/10.1007/s12117-025-09557-5
3. Alonso Berbotto A, Chainey S (2022) A structured methodical process for populating a crime script of organized crime activity using OSINT. Trends Organized Crime 25(3):273–301. https://doi.org/10.1007/s12117-021-09428-9
4. Campana P (2020) Human smuggling: Structure and mechanisms. Crime Justice 49(1):471–519. https://doi.org/10.1086/708663
5. Campana P, Antonopoulos GA (2024) A relational approach to organised crime: Introduction to the special issue on crime and networks. *Trends in Organized Crime*. Advance online publication. https://doi.org/10.1007/s12117-024-09534-4

6. Campana P, Meneghini C (2024) Organised crime movement across local communities: A network approach. Trends Organized Crime 27(3):286–313. https://doi.org/10.1007/s12117-024-09531-7
7. Campana P, Varese F (2018) Organized crime in the United Kingdom: Illegal governance of markets and communities. Br J Criminol 58(6):1381–1400. https://doi.org/10.1093/bjc/azy017
8. Campana P, Varese F (2022) Studying organized crime networks: Data sources, boundaries and the limits of structural measures. Social Networks 69:149–159. https://doi.org/10.1016/j.socnet.2020.03.002
9. Dehghanniri H, Borrion H (2021) Crime scripting: A systematic review. Eur J Criminol 18(4):504–525. https://doi.org/10.1177/1477370819850943
10. Europol (2026) *Internet Organised Crime Threat Assessment (IOCTA) 2026*. https://www.europol.europa.eu/
11. Franceschini I, Li L, Bo M (2023) Compound capitalism: A political economy of Southeast Asia's online scam operations. Crit Asian Stud 55(4):575–603. https://doi.org/10.1080/14672715.2023.2268104
12. 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*. Advance online publication. https://doi.org/10.1007/s12117-024-09552-2
13. Hyslip TS (2020) Cybercrime-as-a-service operations. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 815–846). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_36
14. Lazarus S, Chiang M, Dimitrova RS, Thu TT, Essien E (2026) What do we know about human trafficking and scam compounds in Southeast Asia (2020–2025)? A qualitative meta-synthesis of coercive deviant enterprises. Deviant Behav 47(6):1091–1123. https://doi.org/10.1080/01639625.2025.2604138
15. Leukfeldt ER, Holt TJ (2020) Examining the social organization practices of cybercriminals in the Netherlands online and offline. Int J Offender Ther Comp Criminol 64(15):1503–1523. https://doi.org/10.1177/0306624X19895886
16. Leukfeldt ER, Lavorgna A, Kleemans ER (2017) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. Eur J Criminal Policy Res 23(3):287–300. https://doi.org/10.1007/s10610-016-9332-z
17. Lin LSF (2025) Examining the role of deepfake technology in organized fraud: Legal, security, and governance challenges. Front Law 4:6–17. https://doi.org/10.6000/2817-2302.2025.04.02
18. Matthijsse SR, van ' MS, Leukfeldt ER (2023) Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*. Advance online publication. https://doi.org/10.1007/s12117-023-09496-z
19. National Crime Agency (2026) *National Strategic Assessment of Serious and Organised Crime 2026*. https://www.nationalcrimeagency.gov.uk/
20. Office of the United Nations High Commissioner for Human Rights (2023) *Online scam operations and trafficking for forced criminality in Southeast Asia*. https://www.ohchr.org/
21. Sun A, Akartuna EA, Manning M (2026) Employment scams: A crime script and scoping review of prevailing methods, trends and future directions. *Trends in Organized Crime*. Advance online publication. https://doi.org/10.1007/s12117-026-09598-4
22. Tiwari M, Zhou Y, Lee JR, Naraspuram KN, Bewong M, Rathore V (2026) Generative AI and financial crimes: A quantitative systematic literature review. Crime Sci 15., Article 5. https://doi.org/10.1186/s40163-026-00268-y
23. United Nations Office on Drugs and Crime (2023) Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia. UNODC Regional Office for Southeast Asia and the Pacific. https://www.unodc.org/
24. United Nations Office on Drugs 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/
25. United Nations Office on Drugs and Crime (2026) An interconnected criminal ecosystem: Transnational organized crime threat assessment for Southeast Asia 2026. UNODC Regional Office for Southeast Asia and the Pacific. https://www.unodc.org/
26. Visconti G (2026) A review of crime at machine speed: Criminological aspects of artificial intelligence's industrialisation of deception. Sci 8(3). Article 54. https://doi.org/10.3390/sci8030054
27. Zhang Y (2026) AI-driven fraud as an emerging cyber risk: Evidence from a global incident-based analysis. *EDPACS*. Advance online publication. https://doi.org/10.1080/07366981.2026.2631066

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementaryFilesS1S4.pdf