Asian Journal
of Criminal Justice
and Forensic Studies

Vol. 2 | No. 1 | 2026
**Journal homepage:** https://asianjustice.kz/

**UDC** 343.983:303.64
**DOI:** 10.63621/ajcjfs/1.2026.04

**Article's History:**
Received: 07.10.2025; Revised: 04.02.2026; Accepted: 18.03.2026

# Social networks as a tool for detecting organised criminal groups in the Philippines

**Raimundas Jurka***
Mykolo Romerio University,
Vilnius, Lithuania
https://orcid.org/0000-0002-9911-5611

**Suggest Citation:**
Jurka, R. (2026). Social networks as a tool for detecting organised criminal groups in the Philippines. *Asian Journal of Criminal Justice and Forensic Studies*, 2(1), 4-14. doi: 10.63621/ajcjfs/1.2026.04.

**Abstract.** The purpose of the study was to investigate the use of social media by law enforcement agencies to detect and investigate organised crime in the Philippines. The study used a set of complementary methods: an analytical and applied approach based on secondary data analysis, a method of system structural analysis, an analytical and synthetic method, a case study, and a method of analysing social networks. It was proved that Open Source Intelligence and Social Network Analysis were transformed into the basis of the Intelligence-Led Policing strategy. It was determined that such methodological integration allows investigators to convert fragmented digital traces into verified physical coordinates of criminal hubs. This proved the feasibility of switching from traditional mass arrests to a strategy of spot neutralisation of key network nodes (brokers and organisers) identified using centrality metrics. This justified the strategic transition from reactive arrests to point-by-point neutralisation of key network nodes (brokers and organisers) identified through network analysis. In the context of the study, a number of practical recommendations were developed aimed at institutionalising the M-SNOS methodology in law enforcement agencies in the Philippines. The developed practical recommendations summarised the need to institutionalise hybrid counteraction by creating a Joint Digital Intelligence Fusion Centre and reorienting the operational strategy to point-by-point neutralisation of key network nodes. The practical significance of the results lies in the fact that law enforcement organisations and technology platforms (Meta, TikTok) can use them to institutionalise the M-SNOS model and implement the legal and operational protocols necessary for a systematic fight against transnational cybercrime

**Keywords:** cyber slavery; mass victimisation; criminal dynamics; digital platforms; digital footprints; syndicate

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

## Introduction

The Philippines faces the challenge of transnational organised crime, including human trafficking, drug trafficking, and cyber fraud, with these groups using social media platforms such as Facebook, TikTok, and Telegram to coordinate, recruit, and launder funds. Traditional intelligence and law enforcement methods were not sufficient to counter these highly adaptive network structures. Thus, there was a need to explore innovative tools for analysing the array of public and semi-closed data from social networks (OSINT – Open-Source Intelligence), as it will provide law enforcement agencies in the Philippines with a methodological basis for identifying and predicting the activities of organised crime groups (OCG) in the digital space.

Research conducted by B.G. Hababag *et al.* (2024), which focused on the analysis of hijacking incidents carried out by the Abu Sayyaf Group (ASG) (Philippines), revealed an understanding of their operational dynamics: centrality measurements identified one node with the greatest impact and another, proactive, indicating a hierarchical but dynamic structure of ASG operations. The identification of social communities confirmed that the abductions were carried out by groups, not individuals, indicating a reorientation of the Philippines national security strategies. Research by S. Donny & N. Zulkifli (2025) focused on assessing the impact of human trafficking and money laundering in the stability and security discourse of the Philippines and Malaysia, using the concept of National Security. The researchers examined the effectiveness of measures implemented by the governments of both countries (legal reforms, regional cooperation), and pointed out the need to strengthen international cooperation, which was important for overcoming crimes that undermine the legal system. W. Duan Xiong & Y.W. Chong (2024), using the technology of data extraction from social networks (SNDM – Scanning Nonlinear Dielectric Microscopy) for comprehensive crime analysis, determined that the use of mining associative rules, cluster analysis, and community detection allows clearly revealing the communication methods and organisational structure of criminal networks. The researchers also built a model for predicting crime trends, which provided public security agencies with timely warning signals to predict the activities of transnational organised crime groups operating, in particular, in the Philippines.

Results of research by K. Zhao *et al.* (2024) confirmed the effectiveness of the Social Network Forensic Analysis model, which uses network representation training to deal with complex criminal networks. The study showed that the model proved its ability to accurately vectorise nodes (using Deepwalk, Line, and Node2vec algorithms), which ensures the preservation of both structural information and properties of the nodes themselves. In addition, the use of modified random wandering and hierarchical clustering improved the accuracy of relationships between nodes and optimised clustering, which allows identifying key figures, leadership structures, and establishing a hierarchy of influence in criminal networks. In addition, the study by F.H. Troncoso & R. Weber (2024) introduced the StPro model for identifying members of a criminal organisation, starting with only one known suspect. The application of the model demonstrated high efficiency, which confirmed the ability of StPro to support criminal investigations, especially in the initial stages, in the case of kidnappings and other violent crimes in the Philippines.

The study by A. Fernández-Planells *et al.* (2021) highlighted the importance of social media in gang lifestyles. The researchers suggested that social networks can be an effective tool in criminal investigations, in particular in the Philippines, as they allow identifying communication patterns and uncovering gang members. The results of the study pointed to the development of a new research question around the topic of social media use by street youth groups. The publications were found to have a variety of topics, methods, samples, and ethical protocols, reflecting the multifaceted nature of online gang activity. The study by Y. Hsiao *et al.* (2023) proved that online conflicts between gang members were not random, but target network relationships that were critically dependent on offline geographical relationships and the history of shootings. A key finding was that statistical associations were based on culturally specific language (gang names, symbols), which was crucial for criminal investigations in gang-related cases in the Philippines, as it highlights the need for mixed methods and qualitative analysis to verify big data. Analysis of social networks by D. Lebert (2025) showed that criminal investigations, reflecting relationships within criminal networks, reveal key players and hidden connections. This method helps law enforcement agencies to target organised crime more effectively.

The analysed studies focused on individual cases (kidnappings, specific gangs) or theoretical / model aspects (node vectorisation, linear identification models). The gap was the lack of a comprehensive, standardised methodological framework that would integrate effective OSINT and SNA (Social Network Analysis) tools, adapt them to the communication features of Philippine organised crime groups in specific, highly adaptive digital environments, and provide Philippine law enforcement agencies with practical recommendations for systematic detection, forecasting, and dismantling of heterogeneous transnational organised crime groups (for example, a combination of drug trafficking and cyber fraud). Therefore, the purpose of the study was to investigate the use of social networks and digital intelligence tools to identify and investigate the activities of organised criminal groups in the Philippines. The goal included the following tasks: to analyse the features of the use of social media (Facebook, TikTok, Telegram) by organised criminal groups in the Philippines for coordination, recruitment, and money laundering; to substantiate the integration of SNA and OSINT methods to create a model for accurate identification of key figures and hierarchical structure of criminal networks; to develop practical recommendations for the use of the analysed methodologies for law enforcement agencies in the Philippines.

## Materials and Methods

This study was analytical and applied, based on secondary data analysis, combining an assessment of digital threats with the development of practical recommendations for improving the work of Philippine law enforcement agencies. The collection of materials for the study was based on the principle of multi-source (triangulation), combining official reports, and case studies illustrating the relationship between digital space and physical crimes.

The study used a set of complementary methods, which provided a systematic approach to the analysis of criminal networks. The method of secondary analysis of empirical data was used to analyse reports by S. Howe (2025), Philippines suspected digital fraud… (2025), Philippines: Global Organised Crime Index (2025). The criterion for selecting these materials was the relevance of the data (2024-2025) and their focus on quantitative verification of criminogenic dynamics, in particular, indicators of digital fraud and socio-demographic characteristics (age, level of mobile penetration). This method was used for quantitative verification of criminogenic dynamics. The system and structural analysis method and the analytical synthetic method were used to substantiate the integration of SNA and OSINT into the M-SNOS (Modified Strategy for Evaluating Online Sources) models. These methods allowed breaking down the complex architecture of transnational cybercrime (professionalisation, migration to Telegram) into functional elements and creating a model of digital OCG exploitation in the Philippines.

The case study method was used to confirm the effectiveness of the Intelligence-Led Policing (ILP) strategy in practice. Case analysis of Philippines rescues more than 1,000... (2023), C.L. Caliwan (2024), Business & Human Rights Resource Centre (2025) was conducted to establish causal relationships between digital intelligence (pattern detection, content geolocation) and the physical elimination of criminal hubs. The selection of cases was carried out according to the criterion of evidence: situations demonstrating the convergence of OSINT (detection of patterns, geolocation of content) and SNA (identification of hierarchy) as a success factor in eliminating physical crime centres were analysed. The social network analysis (SNA) method provided a theoretical rationale for the strategic transition of Philippine law enforcement agencies to ILP tactics involving the neutralisation of criminal network nodes. The effectiveness of this strategy was confirmed by practical cases where social networks (Facebook, Telegram, TikTok) have become a source of intelligence information. The analysis was carried out based on analytical materials (United Nations Office on Drugs and Crime, 2024; Telegram fueling crime..., 2024; Suspected digital fraud rate..., 2025). In cases of liquidation of hubs related to human trafficking and cyber fraud, data from these platforms were used to identify recruitment patterns and geolocation of physical centres.

The results of the analysis were interpreted as evidence of the completion of the structural transformation of crime into a model of "cyber slavery" (a hybrid threat combining Human Trafficking and Cybercrime). The key approach was to identify legal conflict and assess the judicial applicability of digital evidence collected by OSINT methods in the context of Philippine laws (Supreme Court of the Republic Philippines…, 2001; Act of the Republic of the Philippines No. 10173, 2012; Act of the Republic of the Philippines No. 10175, 2012). The regulatory framework was selected based on the principle of relevance: only acts directly regulating the collection, processing, authentication, and judicial admissibility of digital evidence (logs, metadata) were considered. Based on this analysis, a number of practical recommendations were developed aimed at institutionalising the M-SNOS methodology and strengthening partnership between the government and key social networks to systematically counter this hybrid threat. The limitations of the study were the use of secondary data, which did not allow for the initial collection of information from closed Telegram groups, where the coordination activity of OCGs was concentrated.

## Results

**Digital landscape, platform ecosystems, and criminal dynamics of the Philippine region.** According to the analytical report by S. Howe (2025), the digital landscape of the Philippines has become an extensive attack surface for organised crime groups. The phenomenon of permanent digital presence (90.8 million users, 122% mobile penetration) combined with the low median age of the population (26.1 years) led to synergistic convergence of risks, creating a favourable basis for precise exploitation of vulnerable groups. According to the report Philippines suspected digital fraud… (2025), the country shows a steady negative trend, exceeding global digital fraud rates for the fifth consecutive year. In 2024, the world's second rate of suspicious digital transactions was recorded (13.4%), exceeding the global average of 5.4%. The high latency and effectiveness of fraudulent schemes was confirmed by the fact that approximately 74% of respondents report attempts at phishing or social engineering. The socio-economic consequences of this phenomenon were devastating: a nominal financial loss of USD 768 was equivalent to a two-month household income, which creates a destructive feedback loop between digital penetration and economic precarity (Suspected digital fraud rate..., 2025). The poverty factor and the imperative of labour migration, especially among foreign Filipino workers (OFW), have turned vulnerable groups into priority targets for exploitation – from financial fraud to recruitment into criminal networks and use as "money mules" to legalise income.

OCG dynamics were characterised by structural professionalisation and transition to an industrial model. Highly qualified human capital (digital marketing specialists, search engine optimisation, data science) was being integrated into criminal hierarchies. Moreover, there was a technological asymmetry: criminals use generative artificial intelligence (Deepfakes) to pass verification on exchanges or create convincing avatars for "romantic scams".

The financial flows of these transactions were masked through the use of stablecoins (mainly USDT on the Tron / TRC-20 blockchain), which allows bypassing traditional bank monitoring (Suspected digital fraud rate..., 2025).

Digital platforms, in particular the Meta (Facebook) and TikTok ecosystems, have become dominant recruitment vectors, replacing traditional methods. The operational algorithm of criminal groups provides for the creation of "fictitious digital legitimacy": the generation of accounts that mimic the activities of licensed immigration consultants, visa agencies, or recruiters under the "study-to-work" schemes (United Nations Office on Drugs and Crime, 2024). This digital infrastructure allows criminal networks to algorithmically target vulnerable groups (job seekers, migrant workers), directing them to the sectors of forced labour, cyber fraud, and sexual exploitation. Analysis of the organisational structure of the exposure of organised crime groups reveals operational stratification: local Filipino actors were involved at the stage of initial contact and recruitment (providing linguistic and cultural trust), while the logistics of traffic and direct management of exploitation centres were controlled by foreign syndicates (mainly citizens of the People's Republic of China (PRC), Thailand, and Vietnam) (Suspected digital fraud rate..., 2025). Such a transnational criminal nexus complicates the investigation and requires the use of network analysis to identify connected brokers operating at the intersection of local and international jurisdictions.

In parallel, there was a migration of OCG infrastructure to encrypted ecosystems. The Telegram platform has become a dominant hub for drug trafficking and human trafficking due to end-to-end encryption (Telegram fueling crime..., 2024). The threat was the movement of compromised data markets (logs marketplace) to closed Telegram channels, which creates a resource base for attacks based on information obtained through infostealer malware. The systematisation of social media use was presented in Table 1.

**Table 1.** Matrix of digital OCG operation in the Philippines (2020-2025)

| Type of OCG crime | Basic use of social media | Key platforms | SNA strategic focus |
|---|---|---|---|
| Human Trafficking / Illegal Recruitment | Targeting and deceiving job seekers (OFWs); exploiting poverty and young demographics. | Facebook, TikTok, promoters of "study-and-work" schemes. | Identification of Degree Centrality of frontline recruiters and brokers (Betweenness). |
| Cyber fraud / Sextortion | Victim targeting, payment collection, money mules recruitment, digital data trading. | Closed communities, Telegram (data markets). | Mapping specialised roles (technical architects, coordinators) and identifying financial nodes. |
| CSEA (Child Sexual Exploitation and Abuse) | Commodification of materials; Financial transactions and monetisation of platforms. | Platforms with a large number of users; Underground markets. | Tracking of financial flows and identification of links between digital intermediaries and intermediaries. |

**Source:** compiled by the author based on the analysis of the Philippines: Global Organised Crime Index (2025), S. Howe (2025)

Analysis of the table has led to the conclusion that criminal groups' digital infrastructure was segmented by operation. Criminals build a two-tiered system: high-traffic public platforms (Facebook, TikTok) were used exclusively as "entry points" for mass recruitment and victim sourcing, while operational activities, financial transactions, and coordination were moved to encrypted ecosystems (Telegram) or closed communities. Consequently, the digital space of the Philippines has become a hybrid threat environment, where a high level of technological adaptation of the population increases vulnerability to transnational organised crime groups. The combination of socio-economic factors (poverty, migration) with the availability of anonymisation tools and artificial intelligence has created an ecosystem of "cyber slavery" and fraud. This crime architecture, which combines public recruitment with encrypted management, makes traditional investigative methods ineffective, making it necessary to implement OSINT and network analysis tools to deanonymise key nodes in criminal networks.

**Methodology for countering OCG based on the M-SNOS model.** In the face of declining effectiveness of conventional intelligence methods through encryption, it was necessary to implement the M-SNOS model, which was based on the integration of Open Source Intelligence (OSINT) and social network analysis (SNA). OSINT serves as a foundation for accumulating publicly available data, where the use of AI tools was mandatory for processing arrays of unstructured data (images, geotags). Aggregated data sets serve as an empirical basis for implementing the SNA methodology, which allows reconstructing the topology of social connections and ensure preventive neutralisation of threats at the point of their generation (Robertson *et al.*, 2025). Methods of cluster analysis and mining of associative rules allow identifying "technical nodes" and "service brokers" who act as architects of the stability of criminal networks. This provides a shift to Intelligence-Led Policing tactics, converting chaotic data into procedurally relevant information.

The effectiveness of this methodology was confirmed by the analysis of a number of operations. In particular, the operation of law enforcement agencies in May 2023 – the elimination of a fraudulent centre in the province of Pampanga, where more than 1,000 citizens from ten Asian countries were held in slavery (Philippines rescues more than 1,000..., 2023). The dynamics of cybercrime were characterised by structural professionalisation and technological asymmetry (the use of data science and deepfakes), which has led to the emergence of a hybrid threat – cyber

slavery, where victims of exploitation were instrumentalised as perpetrators of cyber fraud. This precedent highlighted the role of foreign syndicates in using the Philippines digital infrastructure to deploy global criminal operations. Table 2 presents a structural and functional analysis of the case Philippines rescues more than 1,000… (2023).

**Table 2.** Structural and functional analysis of the case regarding the elimination of a fraudulent centre in Pampanga province

| Analysis parameter | Empirical data of the case (Facts) | Criminological interpretation and significance for research |
|---|---|---|
| Event identification | Special operation of the National Police of the Philippines (PNP) on May 4, 2023 in the city of Mabalakat (Pampanga). Cyber hub shut down, 1,090 people rescued. | A precedent for the large-scale liquidation of an infrastructure facility of transnational organised crime operating under the cover of legal business. |
| Geography and demographics of victims | Multinational composition: Vietnam (389), China (307), Philippines (171), Indonesia (143), and citizens of Nepal, Malaysia, Myanmar, Taiwan. | The multinational composition pointed to the globalised nature of recruitment and well-established logistics channels for the movement of people ("human traffic") within Asia. |
| Recruitment Vector | Use of social networks (Facebook, Telegram) to post job vacancies in call centres with the promise of legal employment and relocation. | Role of digital platforms as a tool for primary victimisation. Criminals exploit the economic vulnerability of victims through the mechanism of "digital deception". |
| Coercion Mechanism | Confiscation of passports, restriction of freedom of movement (closed perimeter), 18-hour working day, threat of physical violence. | Classic signs of human trafficking for the purpose of labour exploitation. Physical control combined with psychological pressure and debt bondage. |
| Nature of criminal activity | Implementation of the "Pig Butchering" (Sha Zhu Pan) scheme: creating fake romantic relationships to attract investments in fake crypto platforms. | Crime convergence: victims of human trafficking were forcibly transformed into perpetrators of cyber fraud. This makes it difficult to qualify their procedural status (criminal vs victim). |
| Organisational hierarchy | Arrest of 12 guards (7 citizens of China, 4 – Indonesia, 1 – Malaysia). | Indicates control of operations by foreign syndicates. The Philippines was used as a "safe haven", while the beneficiaries and organisers were often non-residents. |
| Conclusions for the M-SNOS methodology | The need to identify online recruitment patterns and analyse financial flows from crypto fraud. | Case proved the need to use M-SNOS to destroy not only the financial, but also the recruitment infrastructure of organised crime groups at an early stage (before moving victims). |

**Source:** compiled by the author based on the analysis of Philippines rescues more than 1,000… (2023)

The systematised data showed the completion of the structural transformation of regional crime into a hybrid model of "cyber slavery", the defining feature of which was the convergence of traditional traffic with high-tech fraud. This symbiosis has given rise to the phenomenon of "forced criminality", where victims of exploitation were instrumentalised as perpetrators of cybercrime, which creates a legal conflict and makes it difficult to identify beneficiaries. This modus operandi not only affirmed the Philippines' role as an operational "safe hub" for foreign syndicates, but also demonstrated a technological asymmetry where digital infrastructure serves as a multiplier of criminal influence. These trends highlight the need for a paradigm shift in countermeasures: a transition from exclusively reactive force measures (ex post facto) to preventive digital intelligence within the framework of the M-SNOS methodology, which allows recruitment networks to be de-anonymised at the stage of digital contact, before the victims were physically relocated.

The practical implementation of Intelligence-Led Policing was demonstrated in the case of the elimination of the hub in Paraniak – C.L. Caliwan (2024). Although the operation culminated in a physical assault on Centrium Tower, its success was based on the analysis of digital traces. Social networks Facebook and Instagram served as a basis for creating digital legends (fake profiles of successful models) and recruiting personnel, while dating applications (Tinder, Bumble) served as an entry point for finding victims through the mechanics of "Love Scams". The next step was to isolate the object in secure messengers (Telegram, WhatsApp), where criminals avoided moderation and applied psychological pressure through video calls for final persuasion. The finalisation of the fraud took place on fake investment platforms, where traffic was directed to steal funds, demonstrating a well-established operational migration from public social networks to closed channels of exploitation. In this context, social networks acted as a "double agent" – identifying patterns (analysis of similar profiles of "wealthy models" allowed linking scattered cases of fraud into a single network); geolocation of infrastructure (monitoring of video content ("indecent shows" and streams) that victims were forced to perform allowed investigators to identify interiors and locate the physical office of the criminals). Table 3 demonstrates how the theoretical principles of OSINT and digital intelligence were converted into practical evidence and physical arrests.

**Table 3.** Structural and functional analysis of the case regarding the liquidation of the hub in Paraniak

| Element of the Intelligence-Led Policing strategy | Implementation in the Paraniak case (2024) |
|---|---|
| Digital pattern recognition | Instead of responding to individual complaints, the police analysed an array of fake accounts. Consistency was found: identical communication scripts, similar "rich model" profiles, and identical social engineering techniques that pointed to a single control centre rather than disparate hackers. |
| Content-to-Location correlation | Law enforcement officers used video content broadcast by criminals as a source of intelligence. Analysis of the video background, broadcast IP addresses, and metadata allowed localising the physical address of the studio in the Centrium Tower business centre, linking virtual chat rooms to real rooms. |
| Deanonymisation of the organisational structure | Social networks have become tools that have brought investigators to the top of the hierarchy. Instead of arresting only low-level operatives (CSR), the police identified and detained members of the management – Nan Shan, Detu Su, and Wu Jian Bin. This was made possible by tracking the chain of teams and financial flows from victims to organisers. |
| Moving from Digital to Physical | The case illustrates the main goal of the new strategy: physical elimination of the hub. Blocking social media accounts was a temporary measure. Instead, the raid seized servers, computers, and mobile phones that were the source of evidence ("logs marketplace") for further investigation. |

**Source:** compiled by the author based on the analysis of C.L. Caliwan (2024)

The practical implementation of the Intelligence-Led Policing strategy in this case showed a change in the architecture of countering organised crime: the rejection of situational response in favour of deanonymisation of infrastructure. The ability of the investigation to convert fragmented digital traces – from social engineering scripts to video broadcast metadata – into verifiable physical coordinates was a success factor, allowing neutralising not only the executive staff, but also the syndicate's management. This approach finally transformed OSINT from an auxiliary analytical tool to a basis for conducting force operations, where the priority was not the temporary blocking of virtual assets, but the physical seizure of hardware – the carrier of a legally significant evidence base for prosecution.

Scaling up counteraction requires going beyond military operations. The analysis of the case Business & Human Rights Resource Centre (2025) pointed to the application of this technological approach, supported by public-private partnerships. In January 2025, the Philippine government (through the Department of Migrant Workers – DMW) conducted an anti-fraud operation. Law enforcement agencies working with social networks Facebook and TikTok, based on their algorithms and internal tools, identified suspicious patterns (mass posting of identical advertisements, use of certain keywords, unusual activity of new accounts) faster than conventional investigation method No law enforcement agency can physically remove more than 70,000 advertisements. Only cooperation with platforms that have technological access allowed for large-scale and rapid disorganisation of the criminal network. This operation was aimed at illegal employment of migrant workers who actively used social networks (Table 4).

**Table 4.** Role of social media and the scale of removal of illegal job advertisements in the Philippines

| Platform | Number of deleted posts | Purpose of the crime | Key scheme performers |
|---|---|---|---|
| Facebook (Meta) | 50,220 | Charging high recruitment fees for non-existent or operational jobs. Involvement in human trafficking schemes. | Legal Connect Travel Services, Golden Power SRLS, Alpha Assistenza, and other fraudulent agencies. |
| TikTok | 21,433 | | |
| Overall result | More than 70,000 | Prevent potential exploitation of "thousands" of employees. | |

**Source:** Business & Human Rights Resource Centre (2025)

The scale of the digital sweep conducted in January 2025 confirmed the dependence of transnational crime syndicates on the algorithmic ecosystems of Meta and TikTok as the main recruitment channel. The volume of deleted content showed that conventional methods of law enforcement response were ineffective against automated mass targeting. Successful neutralisation of the threat to thousands of potential victims was made possible only by moving to the direct operational partnership (G2B) model between the government and technology giants. This has created a new standard of counteraction, where platforms were transforming from passive intermediaries into active participants in the security sector, using internal AI tools (Artificial Intelligence) to preventively disrupt criminal networks at the stage of setting traps, which was unattainable for external OSINT monitoring.

**Legal regulation and judicial challenges and practical recommendations for the Philippines.** The effectiveness of using OSINT in the Philippines depends on compliance with the law and ensuring the validity of evidence. The legal framework includes Supreme Court of the Republic Philippines… (2001), Act of the Republic of the Philippines No. 10173 (2012) and Act of the Republic of the Philippines No. 10175 (2012) (Table 5).

**Table 5.** Legal regulation of OSINT in the Philippines

| Legislative Act | Key value for OSINT |
|---|---|
| Act of the Republic of the Philippines No. 10173 | Regulates the collection, processing, and use of personal data. Limits the possibility of uncontrolled data collection, even if it was publicly available. OSINT-investigators must prove that data collection complies with the principles of legality, proportionality, and purpose. |
| Act of the Republic of the Philippines No. 10175 | Defines cybercrimes (including phishing, illegal access to data, cybersex trafficking) and establishes procedures for their investigation. Provides law enforcement agencies with the authority to collect digital evidence, including traffic and subscriber data. |
| Supreme Court of the Republic Philippines | Establishes rules according to which electronic data (including chat logs, emails, videos, OSINT data) can be accepted in court. This requires authentication of evidence and compliance with the chain of custody. |

**Source:** compiled by the author based on Supreme Court of the Republic Philippines… (2001), Act of the Republic of the Philippines No. 10173 (2012), Act of the Republic of the Philippines No. 10175 (2012)

This table systematises the three-level architecture of legal regulation of digital investigations in the Philippines, which defines the limits of legitimacy of OSINT operations. An analysis of legislative acts has shown that the effectiveness of combating cybercrime depends on striking a balance between the expanded operational powers of law enforcement agencies granted by Act of the Republic of the Philippines No. 10175 and the imperatives of personal data protection under the Data Privacy Act, which imposes restrictions even on the collection of publicly available information. The key tool for legalising the collected data was the Supreme Court of the Republic Philippines… (2001), which transform technical information (chat logs, metadata) into admissible court evidence through strict requirements for authentication and chain of custody preservation, confirming the thesis that without procedural validation, OSINT results lose their legal perspective.

The main challenge for investigators using open-source intelligence techniques was to ensure the integrity and procedural admissibility of the evidence collected in court (Robertson *et al*., 2025; Dekens, 2025). The main problem was the risk of violating the Terms of Service (ToS) of social platforms, since many automated tools for mass data collection (Web scraping) technically contradict the rules of the Meta or TikTok ecosystem. Although this method of gathering information was not always classified as illegal under Philippine law, the fact that corporate rules have been violated can be used by the defence to discredit the ethics or legality of the investigation, thereby calling into question the legitimacy of the materials obtained.

Another aspect was the threat of operational security compromise (OpSec), when improper use of OSINT tools leads to disclosure of the true identity or IP address of the investigator (deanonymisation). Such a leak of information not only creates immediate risks to the security of the operation, but can also lead to procedural violations, which will later become the basis for declaring evidence inadmissible. The situation was complicated by the fragility of digital evidence, which was easily modifiable, which requires strict compliance with the chain of custody and authentication procedures. To ensure admissibility in court, investigators must guarantee the integrity of data from the moment it was collected, using cryptographic hash sums to confirm file integrity, and engage computer forensics experts to testify on the reliability of digital logs (Robertson *et al*., 2025; Dekens, 2025). Overall, the successful use of OSINT in the fight against transnational crime in the Philippines requires high legal and technical literacy from law enforcement agencies to effectively balance the speed of information collection and strict requirements for the legality of the evidence base.

Effective implementation of the M-SNOS (OSINT and SNA) model in Philippine law enforcement requires a comprehensive approach focused on institutionalisation, operational strategy, human resources, legal oversight, and international engagement. Institutionalisation of the methodology involves the creation of a Unified Digital Intelligence Fusion Centre (UDIFC) under the auspices of the National Bureau of Investigation (NBI) and the Department of Justice (DOJ). This centralised body should become a single platform for SNA / OSINT, which guarantees interagency coordination and minimises conflicts of jurisdiction. The operational strategy should shift to prioritising Betweenness Centrality. Efforts should focus not on ordinary perpetrators, but on nodes whose removal would cause maximum structural damage to the network, in particular corrupt officials and technical specialists (IT architects) who support cyber fraud. It was necessary to strengthen personnel capacity and specialisation. This includes the introduction of mandatory SNA / SNDM training programmes for analysts covering cluster analysis and centrality metrics. In parallel, certification with Digital Forensics should be provided to all operational personnel to ensure the proper handling and integrity of electronic evidence in accordance with international standards. The success of M-SNOS depends on strict legal oversight and OpSec protocols. Clear internal Operational Security (OpSec) protocols must be developed and a legal oversight body must be established to mandatorily approve data collection methods that use automation and artificial intelligence. This was a safeguard against legal risks and ensures the judicial suitability of the collected evidence. The fight against hybrid transnational crime requires the active use of international cooperation mechanisms (INTERPOL, UNODC) and integration into international legal

frameworks, such as the Global Cross-Border Privacy Rules (CBPR) Forum, to effectively overcome the transnational complexity of criminal networks, in particular Chinese and Mexican cartels.

The results of the study diagnosed the transformation of the Philippines into a global hub of industrialised cybercrime, where the convergence of technologies (AI, cryptoassets) and social vulnerability has formed hybrid threats such as "cyber slavery". Secondary analysis of cases confirmed that effective counteraction against transnational syndicates was ensured exclusively by transitioning to an Intelligence-Led Policing strategy based on the M-SNOS methodology, which allows digital traces to be converted into precise physical coordinates of criminal centres even before the stage of mass victimisation. In this case, scaling success depends on the synergy between the public sector and technology platforms (G2B partnership) to preventively block threats, while the ultimate strategic effectiveness depends on the ability of investigators to legalise OSINT data within the legal framework, ensuring its procedural admissibility.

## Discussion

The results confirmed the completion of the structural transformation of regional crime (in the case of the Philippines) into a hybrid model of "cyber slavery", which correlates with key trends identified by others in related studies. In particular, R. Woźnica (2021) argued that the evolution of international organised crime led to an accelerated transition from rigid hierarchical structures to flexible, decentralised network forms that were more stable and latent. This network architecture, which minimised risks to management, was a factor that made the transnational nature and high efficiency of the "cyber slavery" scheme possible in recruiting victims through social networks. O.V. Tkachova (2022) further systematised these advantages, determining that the high efficiency of TOC (Territorial Organisation of Crime) was ensured by its rapid adaptation, rationality, and priority of minimising risks. The researcher highlighted the trend of TOC transitioning to cybercrime due to the advantages of the digital environment, such as anonymity and uncontrolled activity, which created the conditions for the development of financially secure criminal communities identical to those identified in the current study.

G.N.A Suarmita & H. Purnomo (2024) provided an empirical context in their papers, confirming that cyber fraud and cyber slavery were characterised by technological asymmetry, the use of fake identities, and the disregard for geographical boundaries, which was identical to the challenges that the M-SNOS model was designed to solve in the current study. In the second part of their analysis, the researchers noted that the fight of the Indonesian National Police (POLRI) against this hybrid threat was reduced due to insufficient internal and interagency coordination, which directly justified the need for the current study to create a Joint Digital Intelligence Fusion Centre (UDIFC) to provide the necessary "Triangular Synergy". Ultimately, L.M. Maldonado Ruiz (2025) provided a legal justification, noting that the cross-border nature of cybercrime and its close connection to networks contributed to a high level of impunity (impunidad). This confirmed the importance of the practical recommendations of the current study to constantly update the regulatory framework and ensure the judicial suitability of digital evidence, since without legalising the results of OSINT in the legal field, effective counteraction was legally impossible.

Analysis of the results of the study conducted by R. Hutagalung (2025), confirmed that in the digital age, there were serious risks associated with computer crime (ciberdelitos), which was rapidly evolving, outstripping traditional regulatory requirements. The key finding was that the cross-border nature of these offences and their close connection to organised criminal networks significantly hampered effective criminal prosecution. This has contributed to a high level of impunity (impunidad). Thus, the fight against cybercrime requires constant updating of the regulatory framework, ensuring effective international cooperation, and adopting a multidisciplinary approach that can withstand both the legal and technological complexity of this phenomenon.

Secondary case analysis in the current study proved that traditional methods were ineffective. Instead, the success of liquidation operations was based on the ability of the investigation to convert fragmented digital traces (pattern detection, Content-to-Location on Facebook / TikTok / Telegram) into verified physical coordinates. This confirmed that OSINT / SNA has transformed from an auxiliary analytical tool to a basis for conducting power operations. Thus, V. Akhgar *et al.* (2016) highlighted the role of open source intelligence (OSINT) as a tool for law enforcement agencies to obtain timely information. The researchers testified that OSINT provided access to a wide range of data, from social media information and geolocation data to intelligence from the Dark Web. M. de P. da S. Moraes (2016) confirmed that in the information age, social media has opened up a wide scope for cybercriminals to take advantage of the anonymity of fake profiles, which correlated with the "cyber slavery" pattern found in the current study. In contrast, the researcher stressed the need to integrate Open Source Intelligence tools and principles of psychology, in particular the concept of lateral thinking, to improve the effectiveness of research.

The use of OSINT in virtual social networks opens up new opportunities for generating knowledge and collecting evidence suitable for submission to the court, which was supposed to be a new strategy for detecting cybercrime, using social networks as a key tool. J. Salonen & A. Guarino (2024) stressed that crimes related to cultural values have become transnational in nature and pose a threat to national security, serving as a source of funding for organised networks. The researchers proposed an intelligence methodology based on SNA techniques, which involved creating a hybrid multiplex graph of a social network by combining data from open and classified domains. The use

of SNA and the presented methods of source correlation and link generation helped to effectively identify transnational criminal networks, which was fully consistent with the integration of OSINT / SNA into the M-SNOS model in the current study. Ph. Rosenkranz & W. Honekamp (2022) confirmed that the use of special methods for collecting open data (OSINT) from social networks helped to provide law enforcement agencies with information that was normally only available through measures that required significant interference with fundamental rights. The researchers focused on obtaining open data to determine movement profiles and demonstrated that OSINT from social media was suitable for this purpose, with Instagram and Snapchat showing the greatest potential. These results confirmed the feasibility of using OSINT for geolocation of physical centres of criminal hubs, as was implemented in the analysed cases of the current study.

X. Yuan *et al.* (2021) successfully demonstrated the use of geolocation data from social networks (X) to achieve situational awareness of drug cartel activities. Through temporal and spatial analysis of clusters of named entities, the researchers were able to track important events and identify thematic hot spots in public discussions. This study confirmed the effectiveness of the OSINT methodology for monitoring transnational crime and its ability to convert digital traces into spatial information, despite problems of language ambiguity, which was fully consistent with the results of the current OSINT effectiveness study. N. Soni & R. Poonia (2025) substantiated the need to improve traditional digital forensics by integrating it with artificial intelligence and OSINT, offering a proactive approach to cybercrime investigation that transcends the reactive nature of conventional methods. They showed that OSINT's AI-driven tools made it possible to collect, process, and analyse huge amounts of publicly available data (from the Dark Web, forums) with unprecedented speed and accuracy. This study directly correlates with the hybrid nature of the threats identified in the current study, emphasising that AI technologies were essential for identifying patterns and preventing cyberattacks before they reach a significant scale.

Thus, the synthesis of the results of the current study with the presented studies confirmed the transformation of regional crime into a model of "cyber slavery". This structural change, reinforced by the anonymity of the digital environment and the cross-border nature of crimes, has rendered traditional, reactive law enforcement methods ineffective. The results of the study confirmed the transformation of OSINT / SNA into the basis of the Intelligence-Led Policing strategy. These models provide the conversion of fragmented digital traces into physical coordinates necessary for conducting operations to eliminate criminal cells. Therefore, countering organised crime requires not only the integration of AI for proactive pattern detection, but also addressing systemic challenges of interagency coordination and ensuring the admissibility of OSINT evidence in court, which was a necessary prerequisite for transitioning to a new standard of hybrid countermeasures.

## Conclusions

An analysis of the use of social media by organised criminal groups in the Philippines has shown that the digital landscape has become a global hub for industrialised cybercrime. It was determined that OCGs use a two-tier operating model: public platforms (Facebook, TikTok) were used for mass algorithmic recruitment and creation of "fictitious digital legitimacy" (study-to-work schemes), while operational activities, financial transactions (USDT on TRON / TRC-20) and coordination migrate to encrypted ecosystems (Telegram). The dynamics of OCG was characterised by structural professionalisation and technological asymmetry (involving Data Science, Deepfakes), which led to the emergence of a hybrid threat – cyber slavery, where victims of exploitation were instrumentalised as perpetrators of cyber fraud. The effectiveness of countering transnational syndicates was ensured solely by the transition to an ILP strategy based on the M-SNOS methodology, which allows converting digital traces into exact physical coordinates of criminal centres even before the stage of mass victimisation.

The rationale for integrating SNA and OSINT methods confirmed that the effectiveness of countering transnational syndicates was ensured solely by the transition to the Intelligence-Led Policing strategy. Case analysis proved that social networks were a source of intelligence information: OSINT analysis allows converting digital traces (scam scripts, video broadcast metadata, etc.) into verified physical coordinates of criminal centres, which was unattainable for traditional methods. The key conclusion of the integration of OSINT and SNA was that law enforcement agencies can move from tactics of mass, ineffective, arrests (targeted at performers) to point-by-point neutralisation of key network nodes. The development of practical recommendations showed that the imperative of institutionalising the M-SNOS methodology in the Philippines requires a two-vector approach: the creation of a Joint Digital Intelligence Fusion Centre to ensure interagency coordination and centralised OSINT/SNA analysis; the development and implementation of strict internal operational security protocols to minimise the risks of compromising investigators and ensure the judicial suitability of collected digital evidence. This was necessary to overcome the main challenge – ensuring the judicial suitability of the collected OSINT evidence in the context of Philippine laws (Data Privacy Act, Supreme Court of the Republic Philippines), and to scale preventive counteraction through operational G2B partnerships with technology giants. Further research should focus on developing algorithms for deanonymising cryptoassets (USDT on TRON / TRC-20) and creating models that can predict the migration of recruitment networks to new encrypted ecosystems.

## Acknowledgements

None.

## Funding

None.

## Author Contributions

R. Jurka designed and carried out a full research cycle – from setting objectives and developing a methodology, to collecting and processing data, conducting empirical analysis and verifying results, through to formulating practical recommendations and writing a research paper. The author developed and implemented an integrated M-SNOS methodology, combining OSINT and SNA, and tested its effectiveness on specific case studies in the Philippines.

## Conflict of Interest

None.

## References


[1] Act of the Republic of the Philippines No. 10173. (2012, August). Retrieved from https://privacy.gov.ph/data-privacy-act/.

[2] Act of the Republic of the Philippines No. 10175. (2012, September). Retrieved from https://surl.li/qoudht.

[3] Akhgar, B., Bayerl, P.S., & Sampson, F. (Eds.). (2016). *Open source intelligence investigation: From strategy to implementation*. Cham: Springer. doi: 10.1007/978-3-319-47671-1.

[4] Business & Human Rights Resource Centre. (2025). *Philippines: Over 70,000 illegal job posts targeting prospective migrant workers taken down from Facebook & TikTok; incl. co. responses*. Retrieved from https://surl.li/oplvgg.

[5] Caliwan, C.L. (2024). *99 workers nabbed in Parañaque scam hub raid*. Retrieved from https://surl.li/mymgax.

[6] Dekens, N. (2025). The 13 biggest OSINT investigation challenges. *ShadowDragon Blog*. Retrieved from https://shadowdragon.io/blog/what-are-the-common-struggles-of-osint-investigations/.

[7] Donny, C.E.A.K., & Zulkifli, N. (2025). Organized crime: The comparative analysis of human trafficking and money laundering (case study: Malaysia-Philippines 2018-2022). *International Journal of Social Sciences and Management Review*, 8(3), 18-34. doi: 10.37602/ijssmr.2025.8303.

[8] Duan Xiong, W., & Yu Chong, W. (2024). Research on the application of social network data mining technology in crime analysis and prevention. *Applied Mathematics and Nonlinear Sciences*, 9(1), 1-12. doi: 10.2478/amns-2024-1832.

[9] Fernández-Planells, A., Orduña-Malea, E., & Feixa Pàmpols, C. (2021). Gangs and social media: A systematic literature review and an identification of future challenges, risks and recommendations. *New Media & Society*, 23(7), 2099-2124. doi: 10.1177/1461444821994490.

[10] Hababag, B.G., Alcantara, L.P., Tale, B., & Rogers, J.K. (2024). A social network analysis on Abu Sayyaf kidnappings. *Southeastern Philippines Journal of Research and Development*, 29(2), 211-228. doi: 10.53899/spjrd.v29i2.258.

[11] Howe, S. (2025). Social media statistics in the Philippines. *Meltwater*. Retrieved from https://www.meltwater.com/en/blog/social-media-statistics-philippines.

[12] Hsiao, Y., Leverso, J., & Papachristos, A.V. (2023). The corner, the crew, and the digital street: Multiplex networks of gang online-offline conflict dynamics in the digital age. *American Sociological Review*, 88(4), 709-741. doi: 10.1177/00031224231184268.

[13] Hutagalung, R., & Lubis, R.H. (2025). Triangular synergy model to enhance the Indonesian National Police's (POLRI) strategy in handling human trafficking of cyber-based slavery. *Journal of Information Systems Engineering and Management*, 10(49s), 27-34. doi: 10.52783/jisem.v10i49s.9805.

[14] Lebert, D. (2025). Using social network analysis to combat organized crime. *International Journal on Criminology*, 12(1), 1-18. doi: 10.18278/ijc.12.1.1.

[15] Maldonado Ruiz, L.M. (2025). Criminogenic elements of information technologies and the proliferation of computer crime. *Investigación Tecnología e Innovación*, 17(23), 41-51. doi: 10.53591/iti.v17i23.1945.

[16] Moraes, M. de P. da S. (2016). *Open source intelligence (OSINT) tools in virtual social networks as resources in cybercrime investigations*. (Undergraduate thesis, Faculdades Integradas da Upis (UPIS), Brasília, Brazil). doi: 10.29327/44190052.

[17] Philippines rescues more than 1,000 trafficking victims used to run online scams. (2023). Retrieved from https://www.abc.net.au/news/2023-05-06/philippines-rescues-more-than-1-000-trafficking-victims/102312936.

[18] Philippines suspected digital fraud rate higher than global level for fifth consecutive year. (2025). Retrieved from https://surl.li/lhdfoy.

[19] Philippines: Global Organised Crime Index. (2025). Retrieved from https://ocindex.net/country/philippines.

[20] Robertson, C., Bouchard, M., Whelan, C., & Girn, A. (2025). Untangling SNA: The use and underuse of social network analysis among crime analysts. *CrimRxiv*. doi: 10.21428/cb6ab371.e31eeea5.

[21] Rosenkranz, P., & Honekamp, W. (2022). Determination of movement profiles based on open-source data from social media. In *Mobility in a globalised world 2021* (pp. 247-256). Bamberg: University of Bamberg Press. doi: 10.20378/irb-58356.

[22] Salonen, J., & Guarino, A. (2024). Art crime does not pay: Multiplexed social network analysis in cultural heritage trafficking forensics. In *Proceedings of the 19th international conference on cyber warfare and security* (pp. 617-620). Reading: Academic Conferences International. doi: 10.34190/iccws.19.1.2066.

[23] Soni, N., & Poonia, R. (2025). *Enhancing digital forensics with AI-Driven OSINT: A proactive approach to cybercrime investigation*. doi: 10.21203/rs.3.rs-6581767/v1.

[24] Suarmita, I.G.N.A., & Purnomo, H. (2024). Challenges of hybrid policing in countering online fraud networks: A case study from Sidrap Regency. *Al-Ishlah: Jurnal Ilmiah Hukum*, 27(1), 17-30. doi: 10.56087/aijih.v27i1.442.
[25] Supreme Court of the Republic Philippines No. 01-7-01-SC "Rules on Electronic Evidence". (2001, July). Retrieved from https://www.doj.gov.ph/files/rules%20on%20electronic%20evidence.pdf.
[26] Suspected digital fraud rate in PH exceeds global average for fifth year in a row: Report. (2025). *InsiderPH*. Retrieved from https://surli.cc/goeivu.
[27] Telegram fueling crime in Southeast Asia as criminal networks flourish. (2024). *YouTube*. Retrieved from https://www.youtube.com/watch?v=PkEnYY_7RUk.
[28] Tkachova, O.V. (2022). Transnational crime: Features and basic models. *Theory and Practice of Jurisprudence*, 2(20), 240-251. doi: 10.21564/2225-6555.2021.2.245462.
[29] Troncoso, F., & Weber, R. (2024). The Steiner tree Prosecutor: Revealing and disrupting criminal networks through a single suspect. *PLOS ONE*, 19(12), article number e0312827. doi: 10.1371/journal.pone.0312827.
[30] United Nations Office on Drugs and Crime. (2024). *Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape*. Retrieved from https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.
[31] Woźnica, R. (2021). Organized crime and state capture in the Western Balkans. *Rocznik Instytutu Europy Środkowo-Wschodniej*, 19(4), 287-306. doi: 10.36874/RIESW.2021.4.14.
[32] Yuan, X., Mahabir, R., Crooks, A., & Croitoru, A. (2022). Achieving situational awareness of drug cartels with geolocated social media. *GeoJournal*, 87(5), 3453-3471. doi: 10.1007/s10708-021-10433-2.
[33] Zhao, K., Zhang, H., Li, J., Pan, Q., Lai, L., Nie, Y., & Zhang, Z. (2024). Social network forensics analysis model based on network representation learning. *Entropy*, 26(7), article number 579. doi: 10.3390/e26070579.