Proceedings of ICILLP 2025 Symposium: Digital Governance: Inter-Firm Coopetition and Legal Frameworks for Sustainability
DOI: 10.54254/2753-7048/2025.BR27646

Applying the SARA Model of Problem-oriented Policing to Combat Telecom Fraud: Insights from Shenzhen's Policing Practices

Xinyi Du

School of Management and Economics, Chinese University of Hong Kong, Shenzhen, China
122020039@link.cuhk.edu.cn

Abstract. Telecom fraud, characterized by its non-contact nature, technological adaptability, and transnational reach, poses unique challenges to traditional law enforcement, including difficulties in tracing digital trails, rapid capital transfer, and fragmented inter-agency collaboration. By analyzing the characteristics of telecom fraud—such as technological sophistication, transnationality, and psychological manipulation—and integrating insights from existing literature, it examines how Problem-oriented Policing (POP)'s proactive, problem-specific framework can address inherent challenges like fragmented collaboration and rapid fund dissipation. The research mainly takes Shenzhen as an example and combines relevant police incident cases from other cities in China. The aim is to utilize the problem-oriented policing theory to analyze the issue of telecommunications fraud crimes and based on the analysis results, propose corresponding prevention, governance, and improvement policies. It establishes a connection between the theoretical policing model and the real anti-fraud practice, providing a practical, feasible, and evidence-based model for anti-telecommunications fraud strategies, thereby reducing the crime rate and the harm to society.

Keywords: Problem-Oriented Policing, Telecom Fraud, SARA Model, Public Policy

1. Introduction

Telecommunication fraud involves the use of telecommunications networks and technologies to commit fraud. According to China's Anti-Telecommunication and Network Fraud Law enacted in December 2022, it is defined as "the use of telecommunication network technologies to defraud public or private property through remote, non-contact means with the purpose of illegal possession" [1]. This type of crime has evolved into a sophisticated transnational criminal enterprise, leveraging technologies such as VoIP and AI-driven social engineering to exploit vulnerable groups worldwide, including within China. Statistical patterns reveal a pronounced regional disparity, with southern provinces—including Hunan, Sichuan, and Guangdong—experiencing significantly higher case rates than northern regions [2]. Moreover, young adults are particularly vulnerable; data from Guangzhou police in 2021 indicated that around 63% of victims

© 2026 The Authors. 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/).

DOI: 10.54254/2753-7048/2025.BR27646

were between 18 and 35 years old, many of whom were students or migrant workers suffering substantial financial losses [3].

Traditional reactive policing models have proven inadequate due to jurisdictional barriers that impede cross-border investigations and the rapid adaptation of criminal tactics to new technologies. These limitations underscore the need for innovative frameworks such as POP, which focuses on addressing root causes rather than symptoms. Although recent studies suggest POP holds promise in cybercrime contexts, empirical research on its application in non-Western settings—especially for technology-facilitated crimes—remains scarce. Shenzhen's demographic profile, characterized by its large tech-savvy youth and migrant population with low fraud awareness, presents a critical context for such research.

To address this gap, this study adopts a mixed-methods approach, combining case analysis of Shenzhen police records with multi-source data from fraud detection platforms, university security logs, and community surveys. It examines how the SARA model (Scanning, Analysis, Response, Assessment) can identify fraud hotspots and dismantle criminal infrastructures. The research offers dual contributions: theoretically, it validates the adaptability of POP to cybercrime environments in mainland China, challenging Western-centric paradigms; practically, it proposes a scalable "technology-community-institution" framework to help urban centers combat evolving financial crimes.

2. Literature review

Telecom network fraud has emerged as a pervasive and evolving threat in the digital age, characterized by its non-contact nature, technological sophistication, and transnational reach. Scholarly discourse on this phenomenon has underscored its multifaceted characteristics: fraudsters leverage advanced communication technologies, such as VoIP, social media platforms, and encrypted messaging apps, to target individuals and organizations globally [4]. Research has identified key crime modus operandi, including impersonation scams (e.g., posing as public officials or customer service representatives), investment frauds ("pig butchering" schemes), and phishing attacks, each tailored to exploit psychological vulnerabilities like trust, greed, or fear [5,6].

A central focus of existing literature lies in the challenges of combating telecom fraud, especially structural issues, such as fragmented collaboration between law enforcement agencies, financial institutions, and telecom operators, which further impede effective intervention. Additionally, victimology studies highlight that susceptibility cuts across demographics, with young adults, college students, and even educated individuals falling prey due to limited digital literacy or over-reliance on technological convenience.

Against this backdrop, problem-oriented policing (POP) has gained traction as a strategic framework for addressing complex crime problems. Originating from Herman Goldstein's critique of reactive policing, POP emphasizes identifying underlying causes of specific crimes, analyzing their contexts, and designing targeted, evidence-based interventions [7]. Unlike traditional law enforcement approaches that focus on incident response, POP advocates for a proactive, iterative cycle: scanning for recurring issues, analyzing their root causes, formulating tailored solutions, and assessing outcomes to refine strategies [8]. Focusing on crimes in China, empirical studies have validated its efficacy in reducing localized crime problems, such as drug markets and property theft, by fostering collaboration between police, communities, and relevant stakeholders [9].

The application of POP to telecom fraud, though nascent, reveals promising synergies. Research suggests that POP's emphasis on problem specificity aligns with the diverse and dynamic nature of telecom fraud. For instance, in addressing Order Fraud scams—a prevalent subtype—POP-guided

DOI: 10.54254/2753-7048/2025.BR27646

initiatives might involve scanning crime data to identify high-risk groups (e.g., college students seeking part-time work), analyzing vulnerabilities (e.g., lack of awareness about platform terms of service), and implementing targeted education campaigns or platform policy reforms. Additionally, emerging case studies—such as regional task forces using POP to map fraud networks and disrupt money flows—demonstrate its potential to move beyond reactive enforcement toward systemic prevention.

In summary, while telecom fraud research has extensively documented its complexities and governance gaps, and POP literature has established its value in problem-specific crime reduction, their intersection remains underexplored. Bridging these domains could offer a structured approach to mitigating telecom fraud, leveraging POP's analytical rigor and collaborative ethos to address both immediate threats and their underlying drivers.

3. Methodology and results

3.1. Case study approach

Guangdong Province, which accounts for 10% of the total number of telecommunications fraud cases filed in China, has provided a large amount of data and cases (Figure 1). This study employs a case study method to explore the application of Problem-Oriented Policing (POP) in addressing the issue of telecommunications fraud in Shenzhen of Guangdong province. According to the data statistics from the Shenzhen Anti-Telecommunication Network Fraud Center, the number of calls received by the public for handling telecommunications network fraud in Shenzhen has generally increased since 2024, reaching 29,833 in April 2025, and there were 2,557 reports from the public.

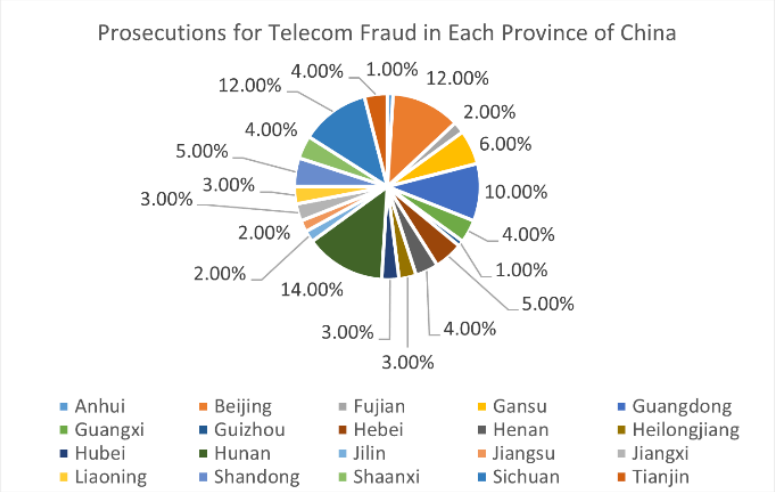

Figure 1. Total statistics of telecommunications fraud cases in all provinces of China

DOI: 10.54254/2753-7048/2025.BR27646

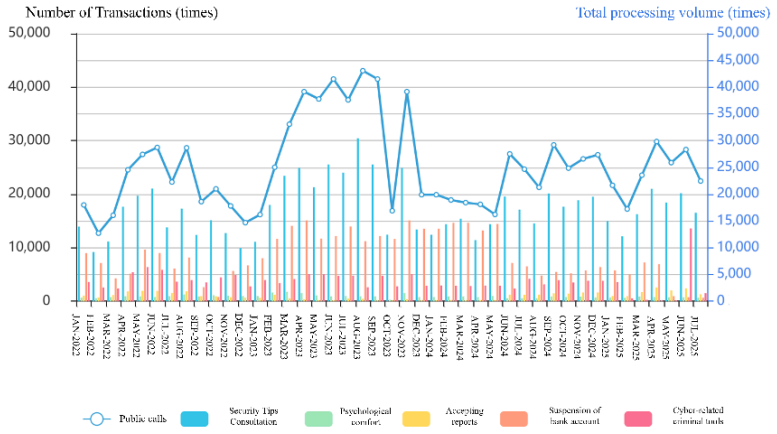

Figure 2. The handling volume of the Shenzhen anti-electronic network fraud center from 2022 to July 2025

Based on this, the case study design is considered appropriate. Shenzhen, as an important technological and economic center in China, has a high incidence of telecommunications fraud (driven by its dense population, extensive digital infrastructure, and frequent cross-border economic activities), making it a highly persuasive case.

The data for this case study were collected from multiple sources to ensure multiple verifications and validity of the data. These sources include official crime statistics and policy documents from the Shenzhen Public Security Bureau; academic research on the trends of telecommunications fraud and law enforcement practices in the Pearl River Delta region; media reports on major fraud cases and law enforcement response measures; and evaluations of local anti-fraud initiatives (such as the "Tianyi Blue Shield" system mentioned by Guangdong Telecom) [10]. The focus of the analysis is to identify the main patterns of telecom fraud in Shenzhen, as well as the potential hotspots and the affected population. It also involves detecting and preventing systemic challenges and evaluating the existing law enforcement intervention measures. This basic analysis provides a foundation for proposing targeted POP strategies using the SARA model.

3.2. Application of the SARA model

3.2.1. Scanning

Scanning work in Shenzhen focuses on identifying high-risk areas and populations through data. The official crime map of the Shenzhen Public Security Bureau in 2021 shows that the hotspots of fraud-related crime cases are mainly located in industrial areas (such as Bao'an District), residential areas with a large number of migrant populations (such as Longgang District and Longhua District), and areas with frequent cross-border business activities. The time pattern indicates that the activity peaks occur on weekends and at night, which is consistent with the increase in personal device usage and the research conclusion of Zhang in 2025 [2]. Furthermore, by analyzing the data processed by the anti-fraud center (Figure 1), it can be observed that the summer months from June to August are usually the peak period for telecommunications fraud each year, which coincides with the period when graduates are seeking employment. The demographic analysis shows that victims aged between 25 and 40, especially students who have just graduated and need employment, unemployed individuals, people with loan needs, and those who frequently use the internet for shopping are the

DOI: 10.54254/2753-7048/2025.BR27646

most vulnerable to investment fraud. These insights from the police database and victim investigations are consistent with the national trend emphasizing digital literacy and the role of the social environment in the victim situation [5].

3.2.2. Analysis

The root causes of Shenzhen's telecom fraud crisis are multifaceted. Technologically, fraudsters exploit the city's advanced digital infrastructure: encrypted messaging apps facilitate anonymous communication, while cross-border payment platforms enable rapid fund dissipation. Systemically, gaps in interagency data sharing—between police, banks, and tech firms—delay fraud detection, as noted in evaluations of the city's anti-fraud command center. Psychologically, scams are tailored to local norms: fake investment schemes often reference Shenzhen's startup culture, promising "tech-driven returns," while impersonation scams capitalize on respect for bureaucratic authority.

Structural factors also play a role. Shenzhen's large transient population, many of whom lack strong social networks, reduces informal guardianship—a dynamic consistent with routine activity theory, which emphasizes the role of social disorganization in crime opportunity [10]. Additionally, the city's status as a financial hub attracts international fraud networks, leveraging its cross-border financial channels to launder funds, as observed in transnational cases documented by local authorities.

3.2.3. Response

Shenzhen's response strategy embodies the problem-oriented policing principle, including targeted law enforcement, technological innovation, and community participation. The police have collaborated with technology giants (such as Tencent and Huawei) to develop an artificial intelligence-based fraud detection system. This system identifies risks in real time by analyzing communication patterns and transaction behaviors. These systems generate alerts at a high frequency every day, enabling proactive measures such as account freezing and user warnings.

Community-based initiatives include conducting "anti-fraud seminars" in technology parks and residential areas, where the police and victims share cases to raise awareness. The city has also expanded its "Shenzhen Energy" network civility public awareness campaign, using social media, subway advertisements, and community broadcasts to disseminate fraud warnings tailored to the local population characteristics. Additionally, institutional reforms have strengthened cross-border cooperation. The Shenzhen police have established joint action teams with the police of Hong Kong and Southeast Asian countries to dismantle cross-border fraud networks.

3.2.4. Assessment

The initial assessment of the Shenzhen strategy has shown encouraging results. According to the 2024 Public-Ministry Communication interview with the Public Security Bureau, in 2023, the number of telecom fraud cases in the city decreased by 8.2%; losses decreased by 24.8%; the number of solved cases of telecom fraud and related crimes increased by 17.0%; and the number of arrested suspects increased by 67.3%, achieving "two decreases and two increases" for three consecutive years [11]. A total of over 360 million yuan in funds was successfully returned, ranking first in Guangdong Province, effectively recovering the economic losses of the public and ensuring the safety of fund usage. However, there are still some challenges: the decline in cases of "pig

DOI: 10.54254/2753-7048/2025.BR27646

slaughtering" fraud (which relies on emotional manipulation) is relatively limited, indicating the need for more detailed psychological intervention measures.

4. Discussion

The findings from the application of Problem-Oriented Policing (POP) and the SARA model to Shenzhen's telecom fraud landscape offer both theoretical and practical insights into combating complex cybercrimes in technologically advanced urban environments.

4.1. Theoretical implications

The study reinforces the utility of POP as a framework for addressing dynamic crime problems like telecom fraud. By focusing on specific scam types (e.g., fake investment platforms, "pig butchering") and their root causes—rather than relying on blanket enforcement—Shenzhen's approach aligns with Goldstein's original vision of problem-oriented policing, which emphasizes tailored interventions based on empirical analysis. The SARA model, in particular, proved valuable in structuring this process: scanning identified high-risk populations and hotspots, analysis uncovered systemic vulnerabilities (e.g., cross-border data gaps), responses integrated technological and community-based solutions, and assessment provided actionable feedback. This structured cycle validates the model's adaptability to digital-era crimes, extending its applicability beyond traditional street-level offenses [12].

Moreover, the findings echo routine activity theory, which posits that crime occurs at the intersection of motivated offenders, suitable targets, and absent guardians. Shenzhen's case illustrates how telecom fraud exploits this triad: motivated transnational networks leverage encrypted technologies, suitable targets (e.g., tech professionals) are identified via data analytics, and guardianship (e.g., rapid fund freezing) is often delayed by fragmented data sharing. For law enforcement, Shenzhen's experience underscores three critical practices. First, interagency collaboration is indispensable. The city's anti-fraud command center, which integrates data from telecom operators, banks, and tech firms, reduced response times and enhanced fund recovery—demonstrating that breaking down silos between public and private sectors is key to countering transnational fraud networks. This aligns with Teng's findings on the limitations of isolated policing efforts in J province, emphasizing the need for systemic coordination [13].

Second, technological innovation must be paired with contextual awareness. Shenzhen's AI-driven alert systems, while effective in flagging suspicious transactions, required continuous refinement to address local scam variants. This highlights the importance of combining advanced tools with on-the-ground intelligence, as rigid technological solutions may fail to adapt to region-specific criminal tactics.

Third, public engagement strategies must be demographically tailored. Shenzhen's "Zhen Energy" campaign, which targeted young professionals with investment scam warnings and older residents with impersonation alerts, improved awareness rates significantly.

4.2. Limitations and future directions

The study's focus on Shenzhen, while informative, limits generalizability. As a global tech hub, the city's digital infrastructure and cross-border dynamics create a unique fraud ecosystem, and strategies effective here may require adaptation in regions with less advanced technological capacity. Additionally, reliance on official crime data and bulletins, while necessary, may undercount

DOI: 10.54254/2753-7048/2025.BR27646

unreported cases—particularly among victims reluctant to disclose financial losses or embarrassment.

Future research should explore two avenues: first, the long-term sustainability of cross-sector partnerships, as maintaining collaboration between police, tech firms, and international agencies requires ongoing resource investment and trust-building. Second, emerging threats such as AI-generated deepfakes and quantum encryption, which could render current detection systems obsolete, demand proactive, problem-oriented adaptations of the SARA model.

In conclusion, Shenzhen's application of POP and the SARA model demonstrates that telecom fraud, despite its complexity, can be mitigated through systematic analysis, targeted innovation, and community collaboration.

5. Conclusion

The study examined the application of Problem-Oriented Policing (POP) and the SARA model in addressing telecommunications fraud in Shenzhen. Findings demonstrate that systematic scanning, analysis, targeted response, and continuous assessment significantly reduce fraud incidence by addressing underlying issues such as data fragmentation, technical vulnerabilities, and group-specific victim patterns. The integration of cross-sector collaboration, AI-enhanced detection, and tailored public engagement proved effective in curbing investment scams and improving fund recovery rates, confirming that proactive problem-solving outperforms reactive law enforcement in combating digital crime.

The study extends POP theory into under-researched domains—cross-border telecom fraud and technologically evolving crimes—by illustrating the adaptability of the SARA model and emphasizing iterative evaluation and institutional learning.

Practically, this research offers actionable strategies for policymakers and law enforcement, underscoring the need for sustained interagency cooperation, context-aware technology, and demographically tailored awareness campaigns. These approaches are transferable to other technology-intensive urban regions facing analogous threats.

Limitations include a geographical focus on one city and reliance on official data, potentially overlooking unreported cases. Future studies should conduct cross-regional comparisons, integrate victim surveys, and explore emerging technologies such as blockchain for transaction tracing.

Overall, this research affirms POP's value in countering digital-age crime through a framework that merges technological innovation with community engagement, contributing to more resilient and adaptive fraud governance systems.

References

[1] Wang, A.L.(2022) Interpretation and Application of the Anti-Electronic and Network Fraud Law of the People's Republic of China, China Democracy and Legal Press, Beijing

[2] Zhang, W.R. and Mo, W.X. Analysis and Prevention Research on Telecom Fraud Behaviors [J]. Forest Public Security, 2025, (01): 14-17.

[3] Li, B.B. Research on the Governance of Telecom Fraud in City G of Guangdong Province [D]. Guangdong University of Finance, 2022. DOI: 10.27734/d.cnki.ggdsx.2022.000984.

[4] Jin, X. The Challenges and Breakthroughs in Combating Telecommunication Fraud Crimes [D]. China University of People's Police, 2021. DOI: 10.27634/d.cnki.gzrgu.2021.000258.

[5] Zhang, H. and Jiang, Y. Causes and Countermeasures of Telecommunication Fraud Victims from the Perspective of Criminal Science Theory [J]. Journal of Bohai University (Philosophy and Social Sciences Edition), 2023, 45(03): 38-41. DOI: 10.13831/j.cnki.issn.1672-8254.2023.03.018.

DOI: 10.54254/2753-7048/2025.BR27646

[6] Xie, C.X.H. Analysis of College Telecom Network Fraud Cases and Research on Prevention Countermeasures [J]. Journal of Civil Aviation University of China, 2023, 34(02): 64-67.
[7] Hinkle J C, Weisburd D, Telep C W, et al. When is problem-oriented policing most effective? A systematic examination of heterogeneity in effect sizes for reducing crime and disorder [J]. Policing: A Journal of Policy and Practice, 2024, 18: paae053.
[8] Hinkle J C, Weisburd D, Telep C W, et al. Problem-oriented policing for reducing crime and disorder: An updated systematic review and meta-analysis [J]. Campbell systematic reviews, 2020, 16(2): e1089.
[9] Qi, W.W. Thoughts on Preventable Crime Response from the Perspective of Problem-Oriented Policing [J]. Journal of Shandong Police University, 2015, 27(06): 152-158.
[10] Ma, X.C. and Wang, Sh. H. Research on Telecom Network Fraud in China - Analysis Based on CNKI Data (2002-2021) [J]. Network Security Technology and Application, 2022, (07): 144-146.
[11] Shenzhen Municipal People's Government. (2024) Online Interview of Shenzhen Municipal People's Government 2024 Public-Official Communication (Phase 3) - Public Security Bureau https: //www.sz.gov.cn/hdjl/zxft/zqt/fthg/2024/zmt/content/post_11319939.html
[12] Na C. Proactive crime prevention through problem-oriented governance: A case study of South Korea’s recent efforts to tackle new types of fraud [J]. Policing: A Journal of Policy and Practice, 2023, 17: paac080.
[13] Teng, Y.H. Research on the Problems and Countermeasures of Telecommunication Network Fraud Governance in Province J [D]. Jilin University, 2022. DOI: 10.27162/d.cnki.gjlin.2022.005084.