Evolutionary Game Analysis and Optimization of Police-Enterprise Cooperative Mechanism in Telecommunication Network Fraud Governance

Yongzhao Wang, Lijun Zhou, Yue Liu, Bingqing Xie

Abstract—**Telecommunication network fraud, characterized by its prevalence and cross-regional nature, poses a significant threat to the public welfare and undermines social stability. This paper employs evolutionary game theory and numerical simulation methods to investigate the police-enterprise cooperation mechanisms in the governance of telecommunication network fraud and compares the decision-making behavior of the involved parties under static and dynamic punishment mechanisms. The paper reveals the following findings: under the static punishment mechanism, when the difference in return on investment (ROI) between public security organs and enterprises is lower than the losses incurred by choosing non-cooperative strategies, both parties will opt for proactive cooperation. Specifically, when the ROI for enterprises actively cooperating is significantly higher and positive, and the losses incurred by public security organs for passively cooperating are relatively low, the probability of active cooperation between the police and enterprises exhibits periodic oscillation. Furthermore, the implementation of a dynamic performance evaluation mechanism by the government has been shown to lead to a convergence in the probability of proactive strategies adopted by both parties. To effectively address telecommunication network fraud crimes, it is imperative for the government to enhance its punitive measures against public security organs and implement an appropriate punishment mechanism.**

Index Terms—**telecommunication network fraud, police-enterprise cooperation, evolutionary game model, performance evaluation mechanism, dynamic punishment mechanism.**

I. Introduction

TELECOMMUNICATION network fraud, a novel form of criminal activity, exploits digital platforms such as the telecommunication networks to perpetrate fraudulent acts. This type of fraud is characterized by its non-contact nature, enabling it to quickly and covertly target a wide audience through means such as phone calls, text messages, and platforms like WeChat and QQ. In contrast to traditional fraud, which generally requires face-to-face interaction, telecommunication network fraud is not only more economical to execute but also more efficient, employing increasingly sophisticated methods that are difficult to recognize. This type of fraud has become a widespread global issue, threatening personal property security, social trust, and economic growth. The swift advancement of the Internet and mobile communication technologies has significantly facilitated fraudulent activities. According to the Federal Trade Commission (FTC), U.S. consumers suffered losses of up to 8.8 billion due to fraud in 2022, marking an increase of over 30% compared to 2021 [1]. As the country with the highest number of Internet users in the world, China is also confronted with a significant challenge related to telecommunication network fraud. In 2023, Chinese public security organs initiated legal proceedings against 464,000 telecommunication network fraud cases and apprehended 690,000 suspects, underscoring the formidable challenge in addressing this pressing issue [2].

In the ongoing struggle against the proliferation of telecommunication network fraud, both public security organs and telecommunication companies assume substantial responsibilities. However, due to their respective interests and the inherent challenges of practical cooperation, there are frequently instances of inadequate collaboration between law enforcement and enterprises. As communication service providers, telecommunication companies directly correlate their revenue to user engagement. Consequently, excessively tightening communication channels, which may be utilized for fraudulent activities, undoubtedly affects their economic interests. Conversely, public security organs face challenges such as limited police resources, difficulties in cross-regional case coordination, and insufficient technical means when combating telecommunication fraud. Despite the Ministry of Public Security's repeated emphasis on the necessity of enhanced coordination among various departments, public security organs may encounter difficulties in fully investigating telecommunication fraud cases due to performance evaluation pressures and other factors, as these investigations are often intricate and time-consuming. The China Academy of Information and Communications Technology's "2023 Internet Network Security Report" underscores that inadequate information sharing and collaboration represent significant challenges in the governance of telecommunication network fraud, underscoring the imperative for enhanced police-enterprise cooperation to bolster early warning and prevention capabilities [3]. Consequently, the present study will focus on enhancing the willingness of police-enterprise cooperation and explore the establishment of a more efficient

Manuscript received February 25, 2025; revised April 27, 2025. This work was supported in part by Henan Provincial Soft Science Research Program Project under Grant 252400410565, General Research Project in Educational Science Planning of Henan Province under Grant 2025YB0173, and Research and Practice Project on Educational Teaching Reform at Anyang Normal University under Grant ASJY-2024-AZD-012.

Yongzhao Wang is an associate professor of the School of Mathematics and Statistics, Anyang Normal University, Anyang, 455000, China (e-mail: wangyongzhao1987@126.com).

Lijun Zhou is a postgraduate student of the School of Mathematics and Statistics, Anyang Normal University, Anyang, 455000, China (e-mail: 3500679658@qq.com).

Yue Liu is a postgraduate student of the School of Mathematics and Statistics, North China University of Water Resources and Electric Power, Zhengzhou, 450046, China (Corresponding author e-mail: 3107661789@qq.com).

Bingqing Xie is a postgraduate student of the School of Mathematics and Statistics, Anyang Normal University, Anyang, 455000, China (e-mail: 739800394@qq.com).

reward and punishment model. The objective is to provide new ideas and solutions for effectively curbing telecommunication network fraud.

The existing research on the governance of telecommunication network fraud has primarily centered on technical prevention, legal regulation, and public awareness campaigns. With respect to technical prevention, researchers have explored methods for identifying and intercepting fraudulent calls and messages using big data analysis and machine learning algorithms [4]. In terms of legal regulation, scholars have analyzed the shortcomings of the existing legal framework in combating telecommunication network fraud and proposed recommendations for improving relevant laws and regulations [5]. Furthermore, enhancing public safety awareness is identified as a pivotal strategy to prevent telecommunication network fraud with related studies underscoring the importance of enhancing public awareness and skills in fraud prevention [6]. However, the intricacy and covert nature of telecommunication network fraud underscores the limitations of a singular governance approach. Specifically, the integration of public security departments' resources and telecommunication companies' resources to establish an effective cooperative mechanism is a crucial issue that necessitates attention. Existing research has scarcely addressed the role mechanism of police-enterprise cooperation in the governance of telecommunication network fraud and how to incentivize such cooperation through reasonable institutional design. The predominant approach in the field of crime governance research employs analytical frameworks, which impedes the effective resolution of intricate systemic issues posed by telecommunication network fraud.

Evolutionary game theory, as an analytical instrument for studying strategic interactions among subjects, possesses the capability to dynamically simulate the learning, adaptation, and evolutionary behaviors of different entities during the course of the game [7], [8], [9]. This capacity to simulate provides novel perspectives for understanding cooperation and conflict within complex systems. Recent studies have employed evolutionary game theory to analyze various aspects of governance, including the strategic interactions among government and enterprises in environmental regulation, revealing the cooperative and competitive relationships essential for effective governance [10]. On the one hand, research has underscored the significance of inter-firm cooperation in collaborative emission reduction strategies within green supply chains under government regulation, as well as the dynamic relationships among stakeholders in environmental pollution control [11], [12]. On the other hand, the role of evolutionary game theory in promoting sustainable development through green innovation strategies has been emphasized, alongside the significance of multi-party cooperation in enhancing governance effectiveness through central inspections and media supervision[13], [14]. Collectively, these papers underscore the efficacy of evolutionary game methods in analyzing the behaviors and strategy evolution of subjects within complex systems, thereby providing valuable references for addressing complex governance issues.

In light of the above, this paper aims to utilize evolutionary game theory to develop an evolutionary game model that examines the interactions between public security organs and telecommunications enterprises. This model will enable a comprehensive analysis of the critical factors affecting the willingness and effectiveness of cooperation between the police and enterprises. Furthermore, the paper will explore how reasonable incentive and constraint mechanisms can promote collaboration between the police and enterprises, thereby enhancing the governance effectiveness against telecommunication network fraud. Utilizing evolutionary game theory, this research endeavors to elucidate the intrinsic motivational mechanisms underpinning police-enterprise cooperation, thereby providing a scientific foundation for governmental entities to formulate efficacious policies, culminating in the enhancement of the governance level of telecommunication network fraud.

II. Evolutionary Game Analysis of Police-Enterprise Cooperation

The determination of telecommunications enterprises to adopt proactive cooperation strategies is contingent upon the active collaboration of public security organs. Both parties operate under the principle of bounded rationality, wherein enterprises evaluate the benefits received against the costs incurred, and public security organs consider the performance evaluation mechanisms of the government. When enterprises face low profits and high costs, and public security organs are under significant pressure from government penalties, this can adversely affect the willingness of both parties to engage in proactive cooperation, leading to the failure of collaborative cooperation in telecommunication network fraud. When both parties confront incomplete information, they will eventually identify suitable strategic behaviors over time through continuous trial and error. Consequently, this paper employs an evolutionary game model to investigate the strategic choices of cooperation between public security organs and enterprises.

A. Basic Assumptions

Hypothesis 1: During the collaborative process of combating telecommunication network fraud, the cooperative entities consist of public security organs and enterprises. Both parties adopt two types of strategies: proactive collaboration and passive collaboration. Let the probability of proactive collaboration by public security organs be x, and the probability of passive collaboration be $1-x$. Similarly, let the probability of proactive collaboration by enterprises be y, and the probability of passive collaboration be $1-y$, where $y \in (0,1)$. Specifically, proactive collaboration by public security organs is characterized by their efforts to more effectively combat telecommunication network fraud. This includes providing sufficient manpower and financial support to enterprises, actively participating in joint investigations, offering enforcement assistance, and ensuring the legality of relevant actions. Proactive collaboration by enterprises is reflected in their active reporting of telecommunication network fraud incidents to public security organs, strengthening internal management, and providing necessary technical support and assistance [15], [16]. Conversely, passive collaboration by public security organs is manifested in their failure to respond promptly and effectively to requests for assistance from enterprises in combating telecommunication network fraud. This lack of initiative results in an inability

to take proactive measures and actions against fraud cases. Similarly, passive collaboration by enterprises is characterized by their failure to report fraud incidents to public security organs in a timely manner, reflecting a lack of responsibility and awareness. The inaction that characterizes this passive behavior engenders an incapacity to institute early warning mechanisms for telecommunication network fraud. Consequently, this results in delayed responses to fraud incidents and heightened risks and losses.

Hypothesis 2: The normal benefits for public security organs and enterprises in combating telecommunication network fraud are denoted as π_1 and π_2, respectively. If public security organs choose to engage in proactive cooperation, they will incur a cooperation cost C_1, which includes increased investment in manpower and material resources, as well as costs associated with information sharing and coordination management. Similarly, if enterprises choose to engage in proactive cooperation, they will incur a cooperation cost C_2, which includes expenses for purchasing security equipment and software, as well as time costs for collaborating with public security organs. Enterprises will also need to bear certain risks, such as providing sensitive data that may potentially lead to business information leakage. However, if both public security organs and enterprises are willing to engage in proactive cooperation, they can gain mutual reputational benefits, including enhanced public recognition for their efforts in combating telecommunication network fraud. Consequently, the reputational benefits for public security organs and enterprises are denoted as S_1 and S_2, respectively. When both parties engage in proactive cooperation, the total revenue obtained is denoted as R_1 and R_2.

Hypothesis 3: Police-enterprise free-riding includes the negative cooperation type of public security organs and the negative cooperation type of enterprises, that is, the opportunism of one party will allow the other party get the free-riding benefit of its positive cooperation [17], [18]. The negative cooperation type of public security organs includes the insufficiency of their own resources and workload, resulting in the public security organs being unable to fully commit to anti-fraud work, making it difficult to realize the leading role in cooperation between the police and enterprises, assuming that the benefits of free-riding for its acquisition are denoted as K_1. The negative cooperation type of enterprises includes the lack of communication and trust in the main body of cooperation, as well as the lack of sufficient technology and resources to actively cooperate in the fight against telecommunications network fraud. It is difficult to realize the value of the leading role in the process of cooperation between the police and enterprises, assuming that the benefits of free-riding for them are denoted as K_2.

Hypothesis 4: The government, as a third party, formulates policies and supervise the work of public security organs in combating telecommunication network fraud, even if it is not directly involved in the game of police-enterprise cooperation, but can indirectly affect the outcome of the game by setting up a punitive mechanism for public security organs. The effectiveness of police-enterprise cooperation is included in the performance appraisal[19]. If the public security organs choose to cooperate negatively, resulting in the deterioration of the effectiveness of police-enterprise cooperation, the public security organs will be subject to performance appraisal penalties, including failure to meet the expected amount of penalties, and losses due to administrative warnings, orders for rectification, and so on.

B. The Construction of Evolutionary Game Model

Based on the above hypotheses, the strategy choices and payoff matrix for the game between public security organs and enterprises can be derived, as shown in Table I.

Based on the payoff values of each decision-maker in Table I, the expected payoff U_{11} for public security organs adopting an active cooperation strategy and the expected payoff U_{12} for adopting a passive cooperation strategy, as well as the average expected payoff U_1 for public security organs, are calculated as follows:

The expected payoff for public security organs adopting an active cooperation strategy is:

$$U_{11} = y(\pi_1+S_1+R_1-C_1)+(1-y)(\pi_1+S_1-C_1-F) \quad (1)$$

The expected payoff for public security organs adopting a passive cooperation strategy is:

$$U_{12} = y(\pi_1 + K_1 - F) + (1-y)(\pi_1 - F) \quad (2)$$

The average expected payoff for public security organs is:

$$\begin{aligned} U_1 &= xU_{11} + (1-x)U_{12} \\ &= xy(R_1 + F - K_1) + x(S_1 - C_1) + yK_1 \\ &\quad + \pi_1 - F \end{aligned} \quad (3)$$

The replicator dynamic equation for public security organs adopting an active cooperation strategy is:

$$\begin{aligned} F_1(x) = \frac{dx}{dt} &= x(U_{11} - U_1) \\ &= x(1-x)[y(R_1 + F - K_1) + S_1 - C_1] \end{aligned} \quad (4)$$

Similarly, enterprises can select the cooperative strategy of active collaboration, represented by the dynamic process $G_1(y)$, thereby achieving a synergy between public security organs and enterprises. The dynamic process of collaborative governance can be organized as follows:

$$\begin{cases} F_1(x) = x(1-x)\big[y(R_1 + F - K_1) + S_1 - C_1\big], \\ G_1(y) = y(1-y)\big[x(R_2 - K_2) + S_2 - C_2\big]. \end{cases} \quad (5)$$

C. Stability Analysis of Evolutionary Game under Static Punishment

1) Stability Analysis of a Single Agent: According to the stability theorem of differential equations, the probability of public security organs adopting an active cooperation strategy reaches a stable state when $F_1(x) = 0$ and $dF_1(x)/dx < 0$. For simplicity, let $H_1(y) = y(R_1 + F - K_1) + S_1 - C_1$. From $H_1(y) = 0$, we can derive: $y^* = (C_1 - S_1)/(R_1 + F - K_1)$. Similarly, the probability of enterprises adopting an active cooperation strategy reaches a stable state when $G_1(y) = 0$ and $dG_1(y)/dy < 0$. Let $H_2(x) = x(R_2 - K_2) + S_2 - C_2$. From $H_2(x) = 0$, we can derive: $x^* = (C_2 - S_2)/(R_2 - K_2)$.Here, we only consider the cases where $C_1 - S_1 > 0$, $C_2 - S_2 > 0$, $R_1 + F - K_1 > 0$, and $R_2 - K_2 > 0$. The analysis of other scenarios is similar.

TABLE I
Police-Enterprise Cooperation Payoff Matrix

Public Security Agencies / Enterprises	**Active Cooperation** (x)	**Passive Cooperation** $(1-x)$
Active Cooperation (x)	$\pi_1 + S_1 + R_1 - C_1$, $\pi_2 + S_2 + R_2 - C_2$	$\pi_1 + S_1 - C_1 - F$, $\pi_2 + K_2$
Passive Cooperation $(1-x)$	$\pi_1 + K_1 - F$, $\pi_2 + S_2 - C_2$	$\pi_1 - F$, π_2

Proposition 1: If $y < y^*$, then $x = 0$ is the evolutionarily stable strategy; if $y > y^*$, then $x = 1$ is the evolutionarily stable strategy.

Proof: Since $H_1(x)$ is an increasing function, we can conclude that when $y < y^*$, $H_1(y) < 0$, which leads to $dH_1(x)/dx < 0$. Therefore, $x = 0$ is a stabilization strategy. When $y > y^*$, $H_1(y) > 0$, which leads to $dH_1(x)/dx < 0$. Thus, $x = 1$ is a stabilization strategy.

Proposition 2: If $x < x^*$, then $y = 0$ is the evolutionarily stable strategy; if $x > x^*$, then $y = 1$ is the evolutionarily stable strategy.

Proof: Since $H_2(x)$ is an increasing function, we know that when $x < x^*$, $H_2(x) < 0$, which leads to $dG_1(y)/dy < 0$. Therefore, $y = 0$ is the the stabilization strategy. When $x > x^*$, $H_2(x) > 0$, which leads to $dG_1(y)/dy < 0$. Thus, $y = 1$ is the stabilization strategy.

2) System Stability Analysis: Let $F(x) = 0$ and $F(y) = 0$ in the above replicator dynamic system. The system has five equilibrium points, denoted as $O(0,0)$, $A(0,1)$, $B(1,0)$, $C(1,1)$, and $D(x_1, y_1)$, where $x_1 = (C_2 - S_2)/(R_2 - K_2)$, $y_1 = (C_1 - S_1)/(R_1 + F - K_1)$.

When $0 < C_2 - S_2 < R_2 - K_2$ and $0 < C_1 - S_1 < R_1 - F - K_1$, it follows that $0 < x_1 < 1$ and $0 < y_1 < 1$, satisfying the above system of equations. At this point, $D(x_1, y_1)$ is the system's equilibrium point.

The local stability of the replicator dynamic system is analyzed using the Jacobian matrix[20], [21]. When the Jacobian matrix J at an equilibrium point satisfies $\det(J) > 0$ and $\mathrm{tr}(J) < 0$, the equilibrium point is an evolutionarily stable point of the system. For x and y, the Jacobian matrix is derived as follows:

The Jacobian matrix J can be expressed as:

$$J = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

where $a_1 = (1-2x)[y(R_1 + F - K_1) + S_1 - C_1], b_1 = x(1-x)(R_1 + F - K_1), c_1 = y(1-y)(R_2 - K_2), d_1 = (1-2y)[x(R_2 - K_2) - C_2 + S_2]$.

The determinant of the Jacobian matrix is:

$$\begin{aligned}\det J =& (1-2x)\big[y(R_1 + F - K_1) + S_1 - C_1\big] \\ & \cdot (1-2y)\big[x(R_2 - K_2) - C_2 + S_2\big] - x \\ & \cdot (1-x)(R_1 + F - K_1)y(1-y)(R_2 - K_2).\end{aligned}$$

The trace of the Jacobian matrix is:

$$\begin{aligned}\mathrm{tr}\, J =& (1-2x)\big[y(R_1 + F - K_1) + S_1 - C_1\big] \\ & + (1-2y)\big[x(R_2 - K_2) - C_2 + S_2\big].\end{aligned}$$

By substituting the five equilibrium points into the expressions for the Jacobian matrix, its determinant, and its trace, we obtain the Jacobian matrix and its stability at these five equilibrium points, as shown in Table II.

The conditions under which public security organs and enterprises operate can be categorized into the following eight scenarios, as discussed below. The specific results are presented in Table III.

(1) Low-medium positive constraints: $C_1 - S_1 < \min\{0, R_1 + F - K_1\}$, $0 < C_2 - S_2 < R_2 - K_2$, indicating that the return on investment for public security organs during active cooperation is positive, while the return on investment for enterprises during passive cooperation is negative. The loss incurred by public security organs is smaller than the loss incurred by enterprises during passive cooperation.

(2) Medium-negative-medium-positive constraints: $R_1 + F - K_1 < C_1 - S_1 < 0$, $0 < C_2 - S_2 < R_2 - K_2$, indicating that the return on investment for public security organs during active cooperation is higher than the loss incurred during passive cooperation, while the return on investment for enterprises during passive cooperation is negative.

(3) Low-negative-high constraints: $C_1 - S_1 < \min\{0, R_1 + F - K_1\}$, $\max\{0, R_2 - K_2\} < C_2 - S_2$, indicating that the return on investment for public security organs during active cooperation is positive, while the return on investment for enterprises during passive cooperation is negative.

(4) Medium-negative-high constraints: $R_1 + F - K_1 < C_1 - S_1 < 0$, $\max\{0, R_2 - K_2\} < C_2 - S_2$, indicating that the return on investment for public security organs during active cooperation is positive, while the return on investment for enterprises during passive cooperation is negative.

(5) Low-low constraints: $C_1 - S_1 < \min\{0, R_1 + F - K_1\}$, $C_2 - S_2 < \min\{0, R_2 - K_2\}$, indicating that the return on investment for public security organs during active cooperation is positive, while the return on investment for enterprises during passive cooperation is negative.

(6) Medium-negative-low constraints: $R_1 + F - K_1 < C_1 - S_1 < 0$, $C_2 - S_2 < \min\{0, R_2 - K_2\}$, indicating that the return on investment for public security organs during active cooperation is higher than the loss incurred during passive cooperation, while the return on investment for enterprises during passive cooperation is negative.

(7) Low-medium-negative constraints: $C_1 - S_1 < \min\{0, R_1 + F - K_1\}$, $R_2 - K_2 < C_2 - S_2 < 0$, indicating that the return on investment for public security organs during active cooperation is positive, while the return on investment for enterprises during passive cooperation is negative.

(8) Medium-negative-medium-negative constraints: $R_1 + F - K_1 < C_1 - S_1 < 0$, $R_2 - K_2 < C_2 - S_2 < 0$, indicating that the return on investment for public security organs during active cooperation is positive, while the return on investment for enterprises during passive cooperation is negative.

Firstly, under the low-negative-high and low-medium-negative constraints, public security organs tend to favor active cooperation to maximize input-output benefits. Enterprises, considering long-term advantages, also incline towards active cooperation. This dynamic leads to a stable game equilibrium point at $(1, 0)$, as seen in Scenarios 3

TABLE II
EXPRESSIONS FOR THE DETERMINANT AND TRACE OF THE JACOBIAN MATRIX AT EQUILIBRIUM POINTS

Equilibrium Point	det J	tr J
$O(0,0)$	$(S_1-C_1)(S_2-C_2)$	$(S_1-C_1)+(S_2-C_2)$
$A(0,1)$	$(R_1+F-K_1+S_1-C_1)(C_2-S_2)$	$(R_1+F-K_1+S_1-C_1)+(C_2-S_2)$
$B(1,0)$	$(R_2-K_2+S_2-C_2)(C_1-S_1)$	$(R_2-K_2+S_2-C_2)+(C_1-S_1)$
$C(1,1)$	$(R_1+F-K_1+S_1-C_1)(R_2-K_2+S_2-C_2)$	$-[(R_1+F-K_1+S_1-C_1)+(R_2-K_2+S_2-C_2)]$
$D(x_1,y_1)$	MN	0

Note: $M=(S_2-C_2)(R_2-K_2+S_2-C_2)/(R_2-K_2)$, $N=(C_1-S_1)(R_1+F-K_1+S_1-C_1)/(R_1+F-K_1)$.

TABLE III
STABILITY ANALYSIS OF EQUILIBRIUM POINTS UNDER DIFFERENT SCENARIOS

Scenario 1: $C_1-S_1<\min\{0,R_1+F-K_1\}, 0<C_2-S_2<R_2-K_2$				**Scenario 2:** $R_1+F-K_1<C_1-S_1<0, 0<C_2-S_2<R_2-K_2$			
Equilibrium Point	det J	tr J	**Stability**	**Equilibrium Point**	det J	tr J	**Stability**
$O(0,0)$	<0	Uncertain	Saddle Point	$O(0,0)$	<0	Uncertain	Saddle Point
$A(0,1)$	>0	>0	Unstable Point	$A(0,1)$	<0	Uncertain	Saddle Point
$B(1,0)$	<0	Uncertain	Saddle Point	$B(1,0)$	<0	Uncertain	Saddle Point
$C(1,1)$	>0	<0	ESS	$C(1,1)$	<0	Uncertain	Saddle Point
				$D(x_1,y_1)$	$>$	0	Center Point
Scenario 3: $C_1-S_1<\min\{0,R_1+F-K_1\}, \max\{0,R_2-K_2\}<C_2-S_2$				**Scenario 4:** $R_1+F-K_1<C_1-S_1<0, \max\{0,R_2-K_2\}<C_2-S_2$			
$O(0,0)$	<0	Uncertain	Saddle Point	$O(0,0)$	<0	Uncertain	Saddle Point
$A(0,1)$	>0	>0	Unstable Point	$A(0,1)$	<0	Uncertain	Saddle Point
$B(1,0)$	>0	<0	ESS	$B(1,0)$	>0	<0	ESS
$C(1,1)$	<0	Uncertain	Saddle Point	$C(1,1)$	>0	>0	Unstable Point
Scenario 5: $C_1-S_1<\min\{0,R_1+F-K_1\}, C_2-S_2<\min\{0,R_2-K_2\}$				**Scenario 6:** $R_1+F-K_1<C_1-S_1<0, C_2-S_2<\min\{0,R_2-K_2\}$			
$O(0,0)$	>0	>0	Unstable Point	$O(0,0)$	>0	>0	Unstable Point
$A(0,1)$	<0	Uncertain	Saddle Point	$A(0,1)$	>0	<0	ESS
$B(1,0)$	<0	Uncertain	Saddle Point	$B(1,0)$	<0	Uncertain	Saddle Point
$C(1,1)$	>0	<0	ESS	$C(1,1)$	<0	Uncertain	Saddle Point
Scenario 7: $C_1-S_1<\min\{0,R_1+F-K_1\}, R_2-K_2<C_2-S_2<0$				**Scenario 8:** $R_1+F-K_1<C_1-S_1<0, R_2-K_2<C_2-S_2<0$			
$O(0,0)$	>0	>0	Unstable Point	$O(0,0)$	>0	>0	Unstable Point
$A(0,1)$	<0	Uncertain	Saddle Point	$A(0,1)$	>0	<0	ESS
$B(1,0)$	>0	<0	ESS	$B(1,0)$	>0	<0	ESS
$C(1,1)$	<0	Uncertain	Saddle Point	$C(1,1)$	>0	>0	Unstable Point
				$D(x_1,y_1)$	<0	0	Center Point

Note: The scenarios where $C_1-S_1>0$ are similar and will not be repeated in this paper.

and 7. However, under medium-negative-high constraints, enterprises may opt for passive cooperation when the costs of cooperation outweigh the benefits, resulting in the system failing to achieve a stable equilibrium, as observed in Scenario 4.

Secondly, under the low-medium-positive and low-low constraints, if the benefits of active cooperation for enterprises exceed the losses incurred from passive cooperation, both public security organs and enterprises tend to actively cooperate, resulting in an ideal cooperative state, as illustrated in Scenarios 1 and 5. Conversely, if the losses from passive cooperation are lower than the difference in input-output benefits of active cooperation, public security organs may choose passive cooperation, leading to a dynamic state, as noted in Scenario 2. Under medium-negative-low constraints, public security organs may opt for passive cooperation to mitigate excessive losses to their own interests, while enterprises adjust their strategies due to increased losses, as shown in Scenario 6.

Finally, under the medium-negative-medium-negative constraints, public security organs will determine their cooperative strategies based on the difference in input-output benefits, regardless of whether enterprises choose active or passive cooperation. Consequently, the strategies of both parties gradually evolve into a dynamic state, as observed in Scenario 8. In summary, the cooperative strategies between public security organs and enterprises are influenced by constraint conditions, the trade-off between benefits and losses, and game equilibrium points, exhibiting complex dynamic evolutionary characteristics.

D. Evolutionary Game Analysis under Dynamic Punishment

Assume that public security organs implement a dynamic punishment mechanism, where the government's punishment level for public security organs is linearly related to the probability $1-x$ of choosing passive cooperation[22], [23]. Specifically, the original fixed penalty amount F is adjusted to $(1-x)F$. Under this condition, the dynamic evolutionary system between public security organs and enterprises can

be expressed as follows:

$$\begin{cases} F_2(x) = x(1-x)\{y[R_1 + (1-x)F - K_1] \\ \qquad + S_1 - C_1\}, \\ G_2(y) = y(1-y)\big[x(R_2 - K_2) + S_2 - C_2\big]. \end{cases} \tag{6}$$

It can be derived that the system has at least four equilibrium points, namely $O'(0,0)$, $A'(0,1)$, $B'(1,0)$, and $C'(1,1)$. Let $x_2 = (C_2 - S_2)/(R_2 - K_2)$ and $y_2 = [(C_1 - S_1)(R_2 - K_2)]/[R_1 - (R_2 - K_2 - C_2 + S_2)F - K_1(R_2 - K_2)]$, where: $0 < (C_1 - S_1)(R_2 - K_2) < R_1 - (R_2 - K_2 - C_2 + S_2)F - K_1(R_2 - K_2)$, and $0 < C_2 - S_2 < R_2 - K_2$.

Under these conditions, $0 < x_2 < 1$ and $0 < y_2 < 1$, and the point $D'(x_2, y_2)$ satisfies $F_2(x_2) = 0$ and $G_2(y_2) = 0$. Therefore, $D'(x_2, y_2)$ is an equilibrium point of the system.

Similar to the steady-state solution method, by taking partial derivatives with respect to x and y, the Jacobian matrix can be expressed as:

$$J = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

where $a_2 = (1-2x)\{y[R_1 + (1-x)F - K_1] + S_1 - C_1\}$, $b_2 = x(1-x)[R_1 + (1-x)F - K_1]$, $c_2 = y(1-y)(R_2 - K_2)$, $d_2 = (1-2y)[x(R_2 - K_2) - C_2 + S_2]$.

The determinant and trace of the matrix are given as follows:

$$\begin{aligned} \det J =& (1-2x)\big\{y\big[R_1 + (1-x)F - K_1\big] + S_1 - C_1\big\} \\ & \cdot (1-2y)\big[x(R_2 - K_2) - C_2 + S_2\big] - x(1-x) \\ & \cdot \big[R_1 + (1-x)F - K_1\big]y(1-y)(R_2 - K_2). \end{aligned}$$

$$\begin{aligned} \operatorname{tr} J =& (1-2x)\big\{y\big[R_1 + (1-x)F - K_1\big] + S_1 \\ & - C_1\big\} + (1-2y)\big[x(R_2 - K_2) - C_2 + S_2\big]. \end{aligned}$$

According to the conditions $D'(x_2, y_2)$ satisfying $F_2(x_2) = 0$, $G_2(x_2) = 0$, and the conditions of Scenario 2, the determinant of the matrix is positive, and the trace of the matrix is less than 0. The local stability of each equilibrium point is shown in Table IV.

TABLE IV
Stability of Equilibrium Points under Dynamic Control

Equilibrium Point	$\det J$	$\operatorname{tr} J$	Stability
$O'(0,0)$	< 0	Uncertain	Saddle Point
$A'(0,1)$	< 0	Uncertain	Saddle Point
$B'(1,0)$	< 0	Uncertain	Saddle Point
$C'(1,1)$	< 0	Uncertain	Saddle Point
$D'(x_2, y_2)$	> 0	< 0	ESS

According to the results in Table IV, the system has a unique evolutionary stable point $D'(x_2, y_2)$. This indicates that under the dynamic punishment mechanism, the probability of active cooperation between public security organs and enterprises will stabilize in the long term through dynamic adjustments. Moreover, public security organs can dynamically adjust the relationships among various variables, thereby reducing the probability of passive cooperation by public security organs. Therefore, from the perspective of government policy formulation, implementing a punishment mechanism for public security organs is an effective measure to reduce telecommunication network fraud.

III. Numerical Simulation and Sensitivity Analysis

This section will focus on studying how changes in system parameters affect the strategy selection of the game subject.

A. Simulation of System Evolution Path under the Static Punishment Mechanism

As previously mentioned, under the static punishment mechanism, the system can exist in eight different states when parameters take on varying values. To further examine the evolutionary pathways of the system under these various punishment mechanisms and to assess the impact of key parameter variations on bilateral strategy choices, this paper will employ MATLAB software to conduct numerical simulations for all eight states. The parameters $C_1, C_2, R_1, R_2, S_1, S_2, K_1, K_2, F$ are set to $10, 9, 5.5, 6, 11, 8, 9, 3, 3$, respectively. Under these settings, they satisfy the conditions of scenario 1, as shown in Figure 1, leading the system to converge to the state (1,1). When the value of F varies from 3 to 2, it satisfies the conditions of scenario 2, and the results are shown in Figure 2. At this point, the evolutionary process of the system exhibits a periodic cycle, suggesting that the system lacks an evolutionary stable point. The specific conditions for the remaining six scenarios can also be simulated but will not be elaborated here.

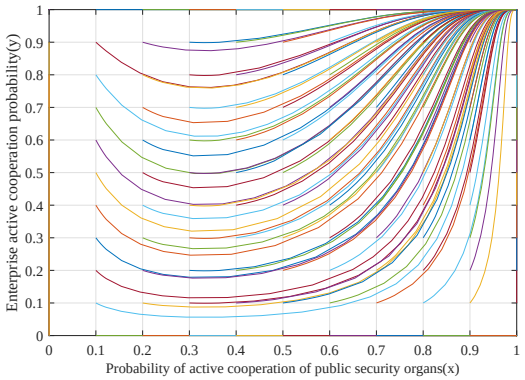

Fig. 1: Evolution Path of Scenario 1.

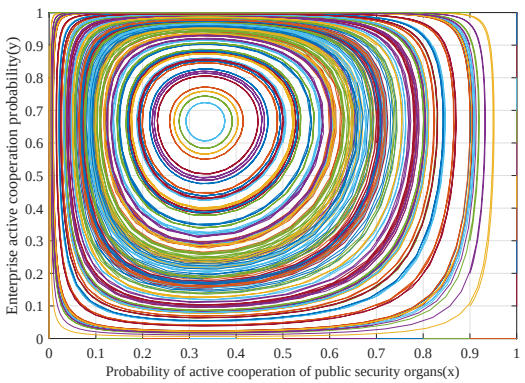

Fig. 2: Evolution Path of Scenario 2.

Due to the differences in investment returns and benefits between public security organs and enterprises, the stability

and speed of returns during active cooperation will vary. This discrepancy not only affects the willingness to cooperate but also plays a significant role in determining the effectiveness and sustainability of the cooperation. Therefore, understanding and reconciling the interests of both parties will be key to achieving long-term effective collaboration.

B. Simulation of Evolutionary Paths under the Dynamic Punishment Mechanism

The evolutionary paths of the system under the dynamic punishment mechanism are simulated. Under the conditions of Scenario 2, assuming that the initial probability of active cooperation between public security organs and enterprises is 0.5, the evolutionary game dynamics of the new system can be obtained. The simulation results are shown in Figures 3 and 4, and a comparison is made with the static scenario.

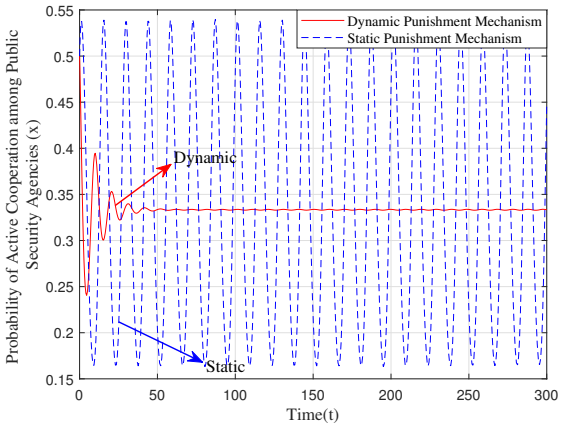

Fig. 3: Behavioral Evolution Path of Public Security Agencies under Different Punishment Mechanisms.

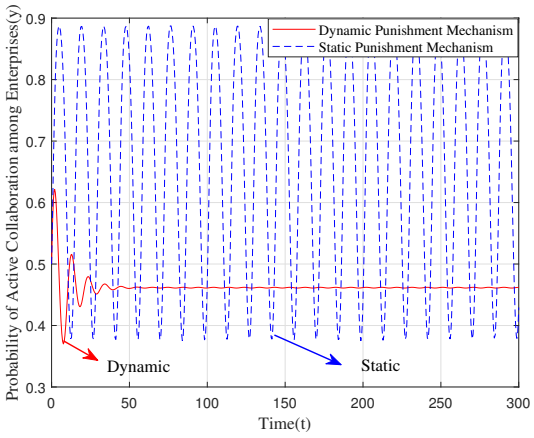

Fig. 4: Evolutionary Path of Positive Behavior of Enterprises under Different Punishment Mechanisms.

As shown in the previous analysis, the evolutionary game stable points of the system under the static and dynamic punishment mechanisms are (x_1, y_1) and (x_2, y_2), with coordinates $(0.33, 0.67)$ and $(0.33, 0.46)$, respectively. From Figures 3 and 4, it can be observed that under the static punishment mechanism, the probability of active cooperation by public security organs, x, and the probability of active cooperation by enterprises, y, exhibit oscillatory fluctuations. Specifically, x fluctuates around 0.33, and y fluctuates around 0.67, but neither shows a trend toward convergence. Under the dynamic punishment mechanism, the probability of active cooperation by public security organs, x, and the probability of active cooperation by enterprises, y, stabilize after a brief period of oscillatory fluctuations. Ultimately, x converges to a stable value of 0.33, and y converges to a stable value of 0.46.

Under the conditions of Scenario 2, the evolutionary path of the system under the static punishment mechanism forms a periodic loop, without a stable equilibrium point, making it difficult for both parties to determine their strategies. When the punishment mechanism is set to dynamic, a new evolutionary game system is constructed. As shown in Figure 5, the evolutionary path of the system exhibits a spiral trajectory, eventually converging to a stable equilibrium point. This indicates that from the perspective of long-term development, the punishment amount imposed by a single public security organ cannot effectively determine the strategies of both parties. However, considering the collective behavior of public security organs as a whole, their decision-making strategies become predictable and stable. From the perspective of higher-level government management, it is necessary for the higher-level government to appropriately adjust the punishment amounts imposed on public security organs during negative management scenarios. This adjustment can increase the probability of public security organs engaging in active cooperation. Therefore, whether from the perspective of the long-term development of public security organs and enterprises or from the perspective of higher-level government management, establishing a dynamic punishment mechanism is an effective approach to promoting active cooperation between public security organs and enterprises.

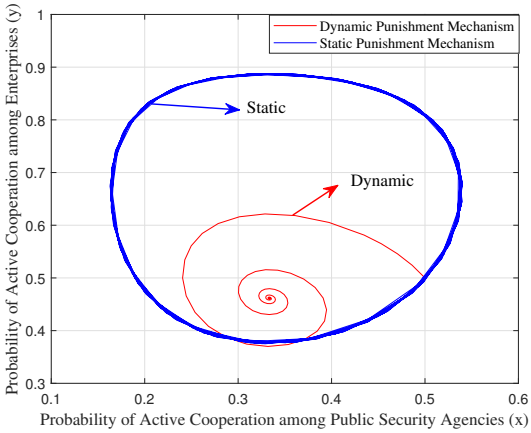

Fig. 5: System Evolution Path under Static and Dynamic Punishment Mechanisms.

C. Sensitivity Analysis

To further investigate the impact of various parameters on the evolutionary paths of the system, in particular the amount of punishment imposed by the government on public security organs, a sensitivity analysis was conducted. Specifically, the effects of changes in F, S_1, and K_1 on the evolutionary

paths of the system were analyzed. The results are shown in Figures 6-8.

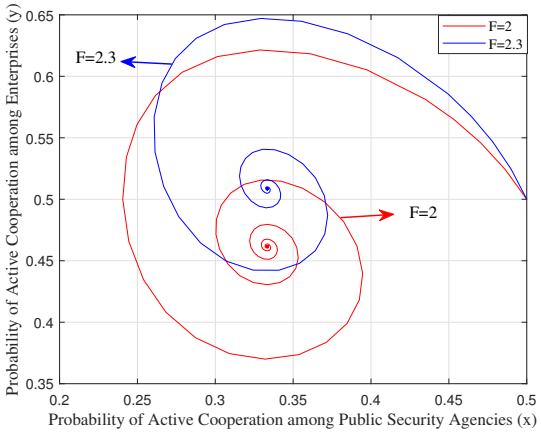

Fig. 6: System Evolution Path under Different Values of F.

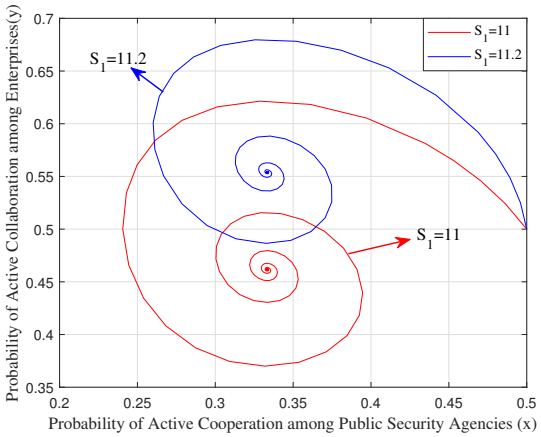

Fig. 7: System Evolution Path under Different Values of S_1.

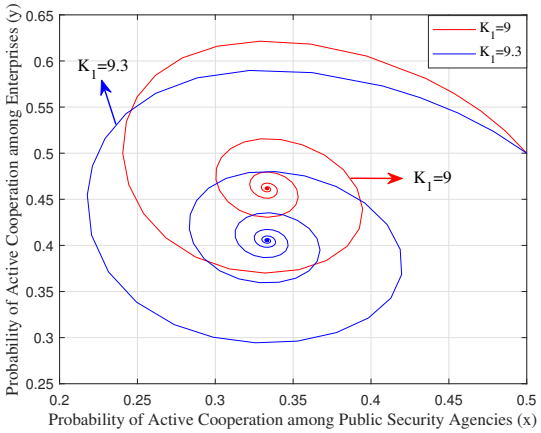

Fig. 8: System Evolution Path under Different Values of K_1.

As shown in Figures 6-8, when the value of F increases from 2 to 2.3, the system's evolutionary stable point shifts from $(0.33, 0.46)$ to $(0.33, 0.51)$. When the value of S_1 increases to 11.2, the system's evolutionary stable point changes from $(0.33, 0.46)$ to $(0.33, 0.55)$. Similarly, when the value of K_1 increases from 9 to 9.3, the system's evolutionary stable point shifts from $(0.33, 0.46)$ to $(0.33, 0.41)$. When the government's punishment for negative cooperation with public security organs increases and the reputation gained from positive cooperation, it will indirectly affect the enterprise's income, and then the enterprise's positive cooperation will increase. Similarly, when the public security organs increase the free-rider benefits of negative cooperation, it will also indirectly affect the overall income of enterprises, and ultimately reduce the probability of enterprises' positive cooperation.

IV. Conclusion and Managerial Implications

A. Conclusions of findings

This study employs the evolutionary game model to investigate the decision-making processes of the two subjects regarding the mitigation of telecommunication network fraud. It uses numerical simulations to compare the evolutionary trajectories under both the static and dynamic punishment mechanisms. Additionally, a sensitivity analysis is conducted to assess the impact of changing a specific variable on the overall evolutionary trajectory of the system. The main conclusions of the study are as follows:

First, under the static punishment mechanism, when the difference in returns from positive cooperation is higher than the loss from negative cooperation, by regulating the relationship between the parameters, the public security organs will be able to cooperate positively, while the enterprises will ultimately choose to cooperate negatively. If the return-return differential of positive cooperation is higher than the loss of negative cooperation, the public security organs will choose negative cooperation to avoid losses, while the enterprises will choose positive cooperation because the loss of negative cooperation is higher than the gain of positive cooperation.

Second, if the additional reputational benefits of positive cooperation are higher than its costs, and the loss of negative cooperation is higher than the return-return difference of positive cooperation, the loss of negative cooperation by public security organs is smaller than the return-return difference of positive cooperation. If a static punishment mechanism is used, there is no fixed decision to stabilise it, and the probability of positive cooperation of both public security organs and enterprises will show cyclical fluctuations in the form of oscillations, but if the government adopts a dynamic punishment mechanism, the probability of the parties involved will converge to a fixed value.

Third, if the difference between the profit and loss of positive cooperation between public security organs is smaller than the loss of negative cooperation, both public security organs and enterprises will choose positive cooperation, regardless of the size of profit and loss of enterprises in positive cooperation.

Finally, as the benefits of the negative cooperation type of free riding by enterprises increase, public security organs will cooperate negatively and enterprises will choose to cooperate positively.

B. Managerial Implications

First, to enhance cooperation incentives between public security organs and enterprises, it is essential to increase the benefits derived from their collaboration and to amplify the additional advantages of active cooperation. Under

conditions of low to medium positive constraints and minimal constraints, both parties will be compelled to choose active cooperation. The government should bolster training and technical support to equip public security organs and enterprises with the specialized knowledge and skills necessary to combat telecommunication network fraud. This will not only enhance their capacity to fight against such fraud but also increase their benefits from participation. By augmenting the benefits of cooperation, the detection rate of telecommunication fraud cases can be significantly improved, enabling public security organs to resolve cases swiftly and apprehend suspects. Furthermore, this approach will facilitate the recovery of some defrauded assets, reduce the incidence of network fraud, and elevate the overall level of network security.

Second, a dynamic punishment mechanism should be established to increase the cost of active cooperation for public security organs while reducing the cost for enterprises. Additionally, dynamic punitive measures should be implemented for instances of negative cooperation. In practice, when negative cooperation by either the government or public security organs leads to financial losses, penalties should be intensified, including substantial financial penalties, to provide an effective deterrent. This aims to standardize cooperative behavior and encourage both agents to actively fulfill their responsibilities.

Finally, the government should integrate punitive mechanisms with routine management to ensure the sustainability of cooperation. In the short term, routine management should be employed to enhance the income of public security organs and enterprises, thereby promoting positive cooperation. When public security organs exhibit negative cooperative behavior, performance evaluations should be conducted to lower their ratings or impose fines and restrictions on resource allocation, complemented by public criticism to damage their reputation. This pressure from public opinion should motivate them to shift towards positive cooperation. Concurrently, the government should establish a data-sharing mechanism with enterprises to facilitate information exchange and monitor anti-fraud activities. Enhancing enterprises' sense of social responsibility through laws, regulations, and industry self-regulation will further improve the efficiency of cooperation and strengthen anti-fraud capabilities.

REFERENCES

[1] Federal Trade Commission, "Consumer sentinel network data book 2022," https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022, 2023.

[2] Ministry of Public Security of the People's Republic of China, "Statistical report on telecommunication network fraud cases in 2023," https://www.mps.gov.cn/, 2024.

[3] China Academy of Information and Communications Technology, "2023 internet network security report," http://www.caict.ac.cn/, 2024.

[4] Yousef A. Yaseen, Malik Qasaimeh, Raad S. Al-Qassas and Mustafa Al-Fayoumi, "Email fraud attack detection using hybrid machine learning approach," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 14, no. 5, pp. 1370–1380, 2021.

[5] Jia Qu, and Hongming Cheng, "Policing telecommunication and cyber fraud: Perceptions and experiences of law enforcement officers in china," *Crime, Law and Social Change*, vol. 82, no. 2, pp. 283–305, 2024.

[6] Qianqian Zhao, Kai Chen, Tongxin Li, Yi Yang, and Xiaofeng Wang, "Detecting telecommunication fraud by understanding the contents of a call," *Cybersecurity*, vol. 1, pp. 1–12, 2018.

[7] Xiaoyan Cao, and Xuelin Zhao, "Tripartite evolutionary game analysis on collaborative governance of compulsory education students' school-work burden," *IAENG International Journal of Applied Mathematics*, vol. 55, no. 5, pp. 1125–1137, 2025.

[8] Yu-Hsien Liao, Chia-Hung Li, Yen-Chin Chen, Li-Yang Tsai, Yu-Chen Hsu, and Chih-Kuan Chen, "Agents, activity levels and utility distributing mechanism: Game-theoretical viewpoint," *IAENG International Journal of Applied Mathematics*, vol. 51, no. 4, pp. 867–873, 2021.

[9] Boontida Uapipatanakul, Jong-Chin Huang, Kelvin H.-C. Chen, Sirawit Ngammuangpak, and Yu-Hsien Liao, "Modeling pollen tube polar growth pattern under asymmetric consideration and creating game-theoretical model for ecotoxicity assessment." *IAENG International Journal of Applied Mathematics*, vol. 55, no. 1, pp. 16–25, 2025.

[10] Zhenhua Zhang, Ke Shi, Yue Gao, and Yanchao Feng, "How does environmental regulation promote green technology innovation in enterprises? a policy simulation approach with an evolutionary game," *Journal of Environmental Planning and Management*, vol. 68, no. 5, pp. 979–1008, 2025.

[11] Hong Huo, Yiwen Lu, and Yue Wang, "Evolutionary game analysis of low-carbon transformation and technological innovation in the cold chain under dual government intervention," *Environment, Development and Sustainability*, pp. 1–28, 2024.

[12] Shaonan Shan, Xia Duan, Wenyan Ji, Tingting Zhang, and Hui Li, "Evolutionary game analysis of stakeholder behavior strategies in 'not in my backyard'conflicts: Effect of the intervention by environmental non-governmental organizations," *Sustainable Production and Consumption*, vol. 28, pp. 829–847, 2021.

[13] Xu Yang, Shan Liao, and Runmao Li, "The evolution of new ventures' behavioral strategies and the role played by governments in the green entrepreneurship context: An evolutionary game theory perspective," *Environmental Science and Pollution Research*, vol. 28, no. 24, pp. 31 479–31 496, 2021.

[14] Mohammad-Ali Eghbali, Morteza Rasti-Barzoki, and Soroush Safarzadeh, "An evolutionary game-theoretic approach for analysis of green innovation and environmental performance of tech firms under stakeholders' policies based on system dynamics," *Clean Technologies and Environmental Policy*, vol. 26, no. 9, pp. 3107–3125, 2024.

[15] Edward Schwarck, "Intelligence and informatization: the rise of the ministry of public security in intelligence work in china," *The China Journal*, vol. 80, no. 1, pp. 1–23, 2018.

[16] Zhichao Zheng, and Shuqi Ma, "Research on international police cooperation from the perspective of foreign-related rule of law-taking lancang-mekong law enforcement and security cooperation as an example," *Journal of Theory and Practice of Social Science*, vol. 4, no. 03, pp. 55–70, 2024.

[17] Yongzhao Wang, Wenqiong Hou, and Bingrui Zhao, "The effect of the alliance between supply members on supply chain performance based on free riding." *IAENG International Journal of Applied Mathematics*, vol. 51, no. 3, pp. 637–644, 2021.

[18] Dongil Chung, Yang-Tae Kim , and Jaeseung Jeong, "Cognitive motivations of free riding and cooperation and impaired strategic decision making in schizophrenia during a public goods game," *Schizophrenia bulletin*, vol. 39, no. 1, pp. 112–119, 2013.

[19] Thomas F. Remington, "Business-government cooperation in vet: a russian experiment with dual education," *Post-Soviet Affairs*, vol. 33, no. 4, pp. 313–333, 2017.

[20] Bogdan M. Wilamowski, Nicholas J. Cotton, Okyay Kaynak, and GÜnhan Dundar, "Computing gradient vector and jacobian matrix in arbitrarily connected neural networks," *IEEE Transactions on Industrial Electronics*, vol. 55, no. 10, pp. 3784–3790, 2008.

[21] Dechao Chen, Yunong Zhang, and Shuai Li, "Tracking control of robot manipulators with unknown models: A jacobian-matrix-adaption method," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3044–3053, 2017.

[22] Xiaoping Wu, and Luyao Jiang, "Evolutionary game research on the decision-making of shared bike placement volume based on dynamic and static punishment mechanisms," *Transportation Planning and Technology*, pp. 1–24, 2024.

[23] André Feliciano Lino, André Carlos Busanelli de Aquino, and Fabricio Ramos Neves, "Accountants' postures under compulsory digital transformation imposed by government oversight authorities," *Financial Accountability & Management*, vol. 38, no. 2, pp. 202–222, 2022.