Hindawi
Discrete Dynamics in Nature and Society
Volume 2022, Article ID 8122630, 14 pages
https://doi.org/10.1155/2022/8122630

Research Article

Study on the Evolutionary Game of Information Security Supervision in Smart Cities under Different Reward and Punishment Mechanisms

Yihang Guo, Kai Zou, Chang Liu, and Yingzi Sun

School of Public Administration, Xiangtan University, Xiangtan 411105, China

Correspondence should be addressed to Yihang Guo; 709069371@qq.com

Received 16 January 2022; Revised 29 March 2022; Accepted 1 April 2022; Published 26 April 2022

Academic Editor: Fahad Al Basir

At present, the information security problems of smart city show a high incidence, and it is necessary to strengthen the information security supervision of smart city. In the process of supervision, there is a game relationship between local government and smart city enterprises. This paper firstly constructs the game matrices of local government and enterprises under the static and three dynamic reward and punishment mechanisms, then conducts numerical simulation with the help of MATLAB to arrive at the optimal reward and punishment mechanism through comparison, and finally explores the influence of the change of the upper limit value of each key variable on the directionality and sensitivity of the decision-making behavior of game subjects under the optimal mechanism. The result shows that initial value is one of the decisive factors influencing the choice of management strategy by enterprise. Dynamic reward and dynamic punishment mechanism is the best reward and punishment mechanism for information security supervision in smart cities. In case the upper limit value of key parameters is increased, a larger punishment has a strong influence on the positive strategy choice of the enterprise, and a reasonable adjustment of the reward policy can likewise mobilize the probability that the enterprise actively chooses to strengthen information security management. Based on the simulation results, we propose a feasible strategy.

1. Introduction

Smart city breaks the traditional urban barriers and obstacles through the intersection and integration of new generation information technologies [1] and is a new urban form that comprehensively improves the modernization, refinement, and science of urban governance [2–6], which provides the first exploration of ideas for future sustainable urban development [7, 8]. Currently, many countries such as the United States, the European Union, and South Korea have put forward strategic initiatives for smart cities [9–11], and their core cities have actively responded to the government's call to join the team to explore the practice of smart city construction. China is not different.

Along with the deepening of smart city construction, the practice of smart cities is increasingly relying on a series of new information technologies such as Internet of Things and cloud computing to achieve and present an irreversible trend. While this trend continues to facilitate people's lives, it also puts the whole urban center in high danger [5], and the information security issue is the most sensitive and vulnerable part of it [12]. According to the "2021 Global Risk Report" released by the World Economic Forum, information security is still one of the major risks of concern, and the percentage of occurrence is increasing year by year. Since 2019 until now, the intervention of many smart city-related technologies has effectively improved the efficiency of epidemic prevention and control but also exacerbated the information security risks due to the COVID-19 virus [13]. Information security is a solid foundation and important guarantee for smart city construction and plays a vital role in social stability and even national security [14]. Although smart cities are public in nature, they are highly dependent on and integrated with enterprises. Therefore, the information security behavior of enterprises is considered as one of the important factors affecting the information security of

smart cities [15, 16]. But the pursuit of profit maximization characteristic of enterprises makes them have the tendency of opportunistic behavior when choosing to strengthen information security management decisions [17], which needs to be guided and regulated by the government. Therefore, handling the conflict and cooperation between the government and the enterprise is the key to guaranteeing the information security of smart cities now.

In recent years, scholars have conducted a lot of research on enterprise information security behavior and government supervision strategy, and the related research mainly includes two aspects: first, the causes of enterprise information security and the influence of government supervision on enterprise information security behavior; second, the use of evolutionary game theory to analyze the relationship between government supervision and enterprise behavior. In terms of the causes of enterprise information security and the impact of government supervision on enterprise information security practices, Malatj et al. [18] and Quinn [19] introduced that most information security problems are caused by human actions or errors within the enterprise. Sengan et al. [20] mentioned that some vendors usually do not evaluate the cybersecurity of software and hardware manufactured for smart cities in order to save costs. Kai et al. [21] elaborated that there are characteristics such as concealment and complexity of information security in smart cities, these characteristics tend to cause information asymmetry, and enterprises can gain illegal profits by taking advantage of their information. Due to the information asymmetry between enterprises and the public and the opportunistic behavior of enterprises, information security supervision is considered to be an effective intervention strategy. The government can set scientific and reasonable reward and punishment policies to intervene and manage the information security behavior of enterprises and prompt them to choose to strengthen information security management strategies. For example, Luning [22] suggested that a possible incentive model in information security supervision is to discipline the subject for improper use of power, to use both encouragement and discipline for responsibility implementation, and to encourage the initiative of obligation implementation. Nepal et al. [23] proposed the possibility of including cybersecurity in the benchmarking analysis within the incentive supervision framework. Can et al. [24] pointed out that the external incentives of legal liability can be used to promote the active legal responsibility of information holders, controllers, and regulators. Herath et al. [25] developed a theoretical model of the incentive effects of punishment, and the severity of punishment was found to have a negative effect on safety behavioral intentions. Yang [26] suggested that a combination of mandatory and incentive regulation can be used to achieve effective supervision of the risk of personal biometric information application.

In terms of using evolutionary game theory to analyze the relationship between government supervision and enterprise behavior, evolutionary game theory [27,28] takes a finite rational game as the analytical framework, and the two sides of the game achieve dynamic equilibrium through the process of continuous learning and adaptation, which makes up for the defects of traditional game theory such as assuming that the participants are perfectly rational and have complete information. In the process of evolutionary game, individuals often dynamically adjust their own strategies based on observing and learning other individuals' strategies. Evolutionary game theory has now been widely used in various types of supervision, such as environmental protection [29], drug quality [30], and information disclosure [31]. Many scholars have extended the game subjects to three or even four parties or optimized the game model by adding governmental reward and punishment mechanisms [32–35]. However, relatively few studies have been conducted on information security supervision using evolutionary game theory, especially in the context of smart cities. Min et al. [36] constructed an evolutionary game model for two groups of overcollecting APPs and the government and concluded that increasing the intensity of punishment by the government could effectively reduce the probability of passive personal data leakage. Xinchi et al. [37] constructed an evolutionary game model of platforms, users, and government and concluded that increasing the penalty for leaking users' private information on platforms is the best strategy to enhance the willingness of platforms to protect users' private information. Kai et al. [38] constructed an evolutionary game model with the smart city operator and the information security regulator as the main players and analyzed the evolutionary stabilization strategies of each game player under six scenarios from the perspective of costs and benefits.

In summary, scholars in various countries have used different theories and based on different models or data to study government policies on enterprise information security behavior. Although this has some reference value, there are still shortcomings: (1) Scholars explain the feasibility of implementing governmental reward and punishment mechanisms in information security supervision. However, from the perspective of research methodology, studies are mostly qualitative and rarely use scientific tools and models to objectively describe and quantitatively prove supervisory issues. In addition, there is less research on the information security behavior of individuals or enterprises and the confrontation, dependency, and constraint relationship between government and enterprises under smart cities. (2) When using evolutionary game theory to explore the issue of information security supervision, some scholars have considered the influence of reward and punishment mechanisms on enterprise information security behavior, but the conclusions seem to differ in terms of implementation effects. Existing studies have more quantification of punishments and less quantification of rewards involved in government interventions. The assumed rewards and punishments are usually static. In fact, government rewards and punishments are not fixed, so it is difficult to reflect the dynamic nature of government reward and punishment mechanisms. The main contributions of this paper are as follows: (1) Using evolutionary game theory, we analyze the impact of different reward and punishment mechanisms on the information security behavior decisions of smart city

enterprises. (2) Using case data from China, we compare the evolutionary results of the system under different reward and punishment mechanisms, combining the simulation results to provide theoretical reference and practical guidance for the government to make regulatory decisions.

The rest of the paper is structured as follows: Section 2 constructs an evolutionary game model of local government and enterprise under the static reward and punishment mechanism and the payoff matrix of both parties. Section 3 discusses the evolutionary stabilization strategies of local government and enterprise under the dynamic reward and static punishment, static reward and dynamic punishment, and dynamic reward and dynamic punishment mechanisms. Section 4 presents a numerical study to test the theoretical results and reveal the mechanism of the parameters' influence on the game process. Finally, Section 5 presents the main conclusions, research limitations, and future research directions.

2. Evolutionary Game Model

2.1. Problem Description and Underlying Assumptions. Information security supervision of smart cities refers to the fact that, in order to cope with the information security problems of smart cities, local governments set up corresponding supervisory agencies to restrict and regulate the information security behaviors of enterprises involved in the construction of smart cities. Therefore, local governments and smart city enterprises are the two main subjects of information security regulation of smart cities, and the discussion of supervisory issues focuses more on these two subjects. For example, in the cybersecurity strategy developed in Singapore, the need to strengthen and expand the regulatory authority of the National Cyber Incident Response Team and the National Cyber Security Centre in smart scenarios was emphasized [39]. The United States constructed a cyber information security sector coordination mechanism to achieve effective regulation of cyber geographic information security, with specific tasks shared by information security-related committees, offices, and administrative agencies at all levels [40]. Like other countries, the Chinese government has established information security supervisory departments such as communication management departments, computer virus prevention and control centers, network security emergency response centers, and disaster recovery centers for critical network systems (usually authorized by government departments to act as government regulators, hereinafter referred to as local governments).

For the local government, the all-round and multidisciplinary supervision is difficult and costly, and it is very easy to have the situation of slack supervision. For the enterprise, the growth in the number of information security incidents and the serious consequences that follow prompted its operational investment had to be raised, but considering the factors of their own operating costs and local government efforts, there will be bad operational speculation, that is, not to strengthen information security management. Therefore, there is an obvious game relationship between the supervision strength of the local government and the degree of operational input of the enterprise, with the former managing and making decisions on the information security of smart cities through supervision and reward and punishment measures and the latter paying more attention to the economic benefits they can obtain in the construction of smart city. Based on the limited rationality of both parties, for the action strategy related to specific information security events, the set of strategies adopted by the local government is {Supervise G_1, Unsupervised G_2}, while the set of strategies that can be adopted by the enterprise is {Manage O_1, Nonmanaged O_2}. The basic assumptions and parameters of the evolutionary model for information security supervision of smart cities are set as follows.

Assumption 1. The probability that the local government chooses the "Supervise G_1" strategy is x, $x \in [0,1]$, and the probability that the local government chooses the "Unsupervised G_2" strategy is $1 - x$; the probability that the enterprise chooses the "Manage O_1" strategy is y, $y \in [0,1]$, and the probability that the enterprise chooses the "Nonmanaged O_2" strategy is $1 - y$.

Assumption 2. When the local government chooses Supervise and the enterprise chooses Manage, the cost of regulation invested by the local government to prevent information security incidents is c_1. Due to the public nature of smart cities, the local government receives a benefit of r_1 as a result of the enhanced management of the enterprise. Due to the proactive strategy adopted by the enterprise, the local government gives the enterprise a corresponding reward [41]. Suppose the reward given by the local government to the enterprise is w and the management cost that the enterprise needs to invest to ensure information security is c_2.

Assumption 3. From the previous analysis, it is clear that the public, as the ultimate benefit subject of smart city, can hardly identify whether the enterprise chooses to manage or not due to the information asymmetry factor and can only rely on the information disclosure of the local government or the information disclosure of the enterprise itself to judge [42]. Therefore, regardless of whether enterprises choose to manage or choose not to manage, the public can only assess the benefits based on their feelings after using smart city services, so the enterprise's benefits are all r_2.

Assumption 4. When the local government chooses Supervise and the enterprise chooses Nonmanaged, the local government takes a penalty measure against the enterprise [43]. Assume that the amount of punishment is f. The probability of an information security event at this time is p_1. The event will cause reputational damage to the local government and the enterprise itself [14, 44], and we assume that the losses caused by the event to the local government and the enterprise are l_1 and l_2.

Assumption 5. When the local government chooses Unsupervised and the enterprise chooses Manage, local governments will not implement incentives for enterprise.

Assumption 6. When the local government chooses Unsupervised and the enterprise chooses Nonmanaged, the local government will not implement punitive measures on the enterprise. At this time, information security incidents will cause social losses [20]. Due to the local government's inaction, it needs to additionally bear the social loss caused by the information security event l_3, and the probability of information security event in this case is p_2; clearly, $p_1 < p_2$.

The parameters are described as shown in Table 1.

The matrix of benefits for the local government and enterprise is shown in Table 2.

2.2. Replication Dynamic Equation. The expected payoff U_{G_1} of the local government when it chooses the "Supervise G_1" strategy is

$$U_{G_1} = y(r_1 - c_1 - w) + (1 - y)(-c_1 + f - p_1 l_1). \tag{1}$$

The expected payoff U_{G_2} of the local government when it chooses the "Unsupervised G_2" strategy is

$$U_{G_2} = yr_1 - (1 - y)p_2(l_1 + l_3). \tag{2}$$

Thus, the local government's average expected payoff is

$$\overline{U_G} = xU_{G_1} + (1 - x)U_{G_2}. \tag{3}$$

The replication dynamic equation of the local government can be further expressed as follows:

$$\begin{aligned} F(x) = \frac{dx}{dt} &= x\left(U_{G_1} - \overline{U_G}\right) \\ &= x(1 - x) \\ &\left(y - w - f + p_1 l_1 - p_2(l_1 + l_3) + f - c_1 - p_1 l_1 + p_2(l_1 + l_3)\right). \end{aligned} \tag{4}$$

Let $F(x) = 0$; we can get $x_1 = 0$, $x_2 = 1$, and $y^* = -(f - c_1 - p_1 l_1 + p_2(l_1 + l_3))/ - w - f + p_1 l_1 - p_2(l_1 + l_3)$.

Similarly, the replication dynamic equation of the enterprise can be further expressed as follows:

$$F(y) = \frac{dy}{dt} = y\left(U_{O_1} - \overline{U_O}\right) = y(1 - y)(x(f + w + p_1 l_2) - c_2). \tag{5}$$

Let $F(y) = 0$; we can get $y_1 = 0$, $y_2 = 1$, and $x^* = c_2/f + w + p_1 l_2$.

The replicated dynamic equation system consisting of the above local government and enterprise is denoted as system 1. If the reward and punishment mechanism of local government is to be effective, the total benefit of enterprise adopting the strategy of "Manage O_1" is greater than the total benefit of enterprises adopting the strategy of "Nonmanaged O_2." The precondition is as follows:

$$r_2 - c_2 + w > r_2 - p_1 l_2 - f. \tag{6}$$

From the above replication dynamic equation, we can get five equilibrium points, namely, (0,0), (0,1), (1,1), (1,0), and (x_1, y_1); the point $(x_1, y_1) = (c_2/f + w + p_1 l_2 - (f - c_1 - p_1 l_1 + p_2(l_1 + l_3))/ -w - f + p_1 l_1 - p_2(l_1 + l_3))$.

2.3. Stability Analysis. According to the method proposed by Friedman [30], the Jacobian matrix can be used to analyze the stability of each equilibrium point. If there exists an equilibrium point that satisfies both its corresponding determinant $tr(J) < 0$ and the trace $de\,t(J) > 0$ in the Jacobian matrix, it is indicated that the equilibrium point is an evolutionary stable strategy (ESS).

The Jacobian matrix of the game system in this paper is as follows:

$$J\begin{bmatrix} (1 - 2x)(y - w - f + p_1 l_1 - p_2(l_1 + l_3) + f - c_1 - p_1 l_1 + p_2(l_1 + l_3)) & x(1 - x)(-w - f + p_1 l_1 - p_2(l_1 + l_3)) \\ y(1 - y)(f + w + p_1 l_2) & (1 - 2y)(x(f + w + p_1 l_2) - c_2) \end{bmatrix}. \tag{7}$$

The stability analysis of each equilibrium point is performed under precondition (1). The $tr(J)$ of points (0,0), (0,1), (1, 1), and (1,0) cannot determine the sign and the $de\,t(J)$ of them are all minus signs. The $tr(J)$ of point (x_1, y_1) is 0 and $de\,t(J)$ is plus sign, as shown in Table 3.

It can be seen that all equilibrium points do not have stability, where the characteristic roots of the point (x_1, y_1) are a pair of purely imaginary roots, which is the only stable equilibrium point of system 1 and does not have asymptotic stability. The evolutionary trajectory of both sides of the game is a closed-loop curve around this point and cannot be stabilized to this point when the system replicates the dynamic phase diagram as shown in Figure 1. The analysis of system 1 by changing the initial variables reveals the following:

(a) When $f - c_1 - p_1 l_1 + p_2(l_1 + l_3) < 0$, the ESS of system 1 is (0,0), at which time the evolutionary stabilization strategies of both sides of the game will tend to {Unsupervised, Nonmanaged}. In this case, the replicated dynamic phase diagram of the system is shown in Figure 2.

(b) When $f - c_1 - p_1 l_1 + p_2(l_1 + l_3) > 0$, the ESS of system 1 is (0,1), at which time the evolutionary

Table 1: Parameter definition.

Parameters	Description
x, y	Strategy options for local government and enterprise.
c_1	Supervision costs invested by the local government to prevent information security incidents, for example, technology costs and human and material costs.
c_2	Operational costs invested by the enterprise to prevent information security incidents, for example, technology costs and management costs.
w	Operating reward from local government when the enterprise chooses Manage, for example, subsidies and tax incentives.
f	Punishment given by the local government when the enterprise chooses Nonmanage, for example, fines and suspension of operations.
l_1	Local government needs to bear losses when they choose Unsupervised, for example, losses from remediation of information security incidents.
l_2	Losses to be borne when the enterprise chooses Nonmanaged, for example, compensation losses and loss of reputation.
l_3	Social losses to be borne by the local government, for example, loss of credibility and compensation for property damage.
r_1	Benefits to local government, for example, reputation enhancement and innovation performance.
r_2	Revenue obtained by the enterprise, for example, product service revenue.
p_1	The probability of an information security incident when the local government chooses Supervise and the enterprise chooses Nonmanaged.
p_2	The probability of information security incidents when the local government chooses Unsupervised and the enterprise chooses Nonmanaged.

Table 2: Game payment matrix between local government and enterprise.

		Enterprise	
		Manage O_1 y	Nonmanaged O_2 $1-y$
Local government	Supervise G_1 x	$(r_1 - c_1 - w, r_2 - c_2 + w)$	$(f - c_1 - p_1 l_1, r_2 - p_1 l_2 - f)$
	Unsupervised G_2 $1-x$	$(r_1, r_2 - c_2)$	$(-p_2(l_1 + l_3), r_2)$

Table 3: Results of stability analysis of system 1.

Equilibrium point	$tr(J)$	Sign	$det(J)$	Sign
(0,0)	$(f - c_1 - p_1 l_1 + p_2(l_1 + l_3)) - c_2$	±	$(f - c_1 - p_1 l_1 + p_2(l_1 + l_3))(-c_2)$	—
(0,1)	$(-w - c_1) + c_2$	±	$(-w - c_1)c_2$	—
(1,0)	$-(f - c_1 - p_1 l_1 + p_2(l_1 + l_3)) + (f + w + p_1 l_2 - c_2)$	±	$-(f - c_1 - p_1 l_1 + p_2(l_1 + l_3))(f + w + p_1 l_2 - c_2)$	—
(1,1)	$-(-w - c_1) - (f + w + p_1 l_2 - c_2)$	±	$(-w - c_1)(f + w + p_1 l_2 - c_2)$	—
(x_1, y_1)	0	0	+	+

stabilization strategies of both sides of the game will tend to {Supervise, Nonmanaged}. In this case, the replicated dynamic phase diagram of the system is shown in Figure 3.

3. Dynamic Reward and Punishment Mechanism

Since there is no ESS in the evolutionary system under the static reward and punishment mechanism, there is no stable equilibrium point that makes the enterprise choose the "Manage O_1" strategy when the initial conditions are changed. Thus, this paper will optimize the original model by adopting the measures of dynamic reward and punishment mechanism for the enterprise and explore whether there exist situations that make the enterprise more likely to choose the "Manage O_1" strategy. Dynamic reward and punishment mechanism means that the strength of reward and punishment changes with the change of enterprise strategy choice. In this paper, the dynamic reward and punishment mechanism is divided into three cases: dynamic reward and static punishment, static reward and dynamic punishment, and dynamic reward and dynamic punishment. Comparing the behavioral strategies of subjects under the four reward and punishment mechanisms, we can get the optimal reward and punishment mechanism.

3.1. Dynamic Reward and Static Punishment. Assume that the reward strength of the local government is linearly related to the strategy choice of the enterprise; that is, $w(y) = y \cdot \overline{w}$, where $\overline{w}$ indicates the upper limit of the reward value, and the punishment value is f constant. When enterprise takes higher probability in the "Manage O_1" strategy, it will get more reward from local government. At this time, the corresponding replication dynamic equation is modified as follows:

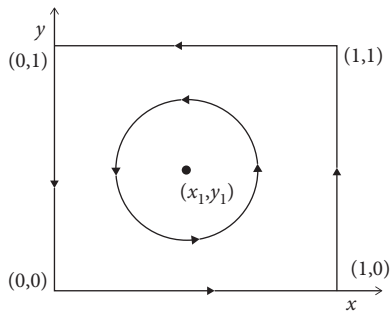

Figure 1: Replicated dynamic phase diagram of system 1 under condition (1).

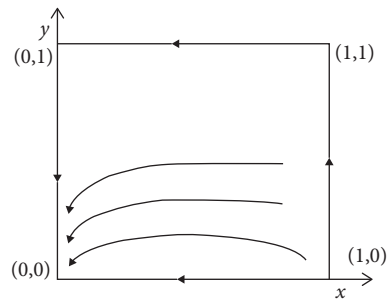

Figure 2: Replicated dynamic phase diagram of system 1 under condition (a).

$$F(x) = \frac{dx}{dt} = x\left(U_{G_1} - \overline{U_G}\right) = x(1-x)(y - w(y) - f + p_1 l_1 - p_2(l_1 + l_3) + f - c_1 - p_1 l_1 + p_2(l_1 + l_3)). \tag{8}$$

Let $F(x) = 0$; we can get $x_1 = 0$, $x_2 = 1$, and $y_1^* = -(f - c_1 - p_1 l_1 + p_2(l_1 + l_3))/ -w(y) - f + p_1 l_1 - p_2(l_1 + l_3)$.

$$F(y) = \frac{dy}{dt} = y\left(U_{S_1} - \overline{U_S}\right) = y(1-y)\left(x\left(f + w(y) + p_1 l_2\right) - c_2\right), \tag{9}$$

Let $F(y) = 0$; we can get $y_1 = 0$, $y_2 = 1$, and $x_1{}^* = c_2/f + w(y) + p_1 l_2$.

The above replicated dynamic equation set forms system 2. We can get five equilibrium points, namely, (0,0), (0,1), (1,1), (1,0), and (x_1, y_1); the point $(x_2, y_2) = (c_2/f + w + p_1 l_2 - (f - c_1 - p_1 l_1 + p_2(l_1 + l_3))/ - w - f + p_1 l_1 - p_2 (l_1 + l_3))$.

The precondition for the effectiveness of the reward and punishment mechanism is as follows:

$$r_2 - c_2 + w(y) > r_2 - p_1 l_2 - f. \tag{10}$$

The stability analysis of each equilibrium point is performed under precondition (2). The $tr(J)$ of the points (0,0), (0,1), (1,1), and (1,0) cannot determine the sign and $de\ t(J)$ are minus signs. The $tr(J)$ of the points (x_2, y_2) is 0 and $de\ t(J)$ is minus sign. It can be seen that all equilibrium points are not stable. In contrast to the static reward and punishment mechanism, the strategy evolution trajectory of local government and enterprises is not a closed-loop curve formed around the point (x_2, y_2), but a closed orbital loop from the starting point.

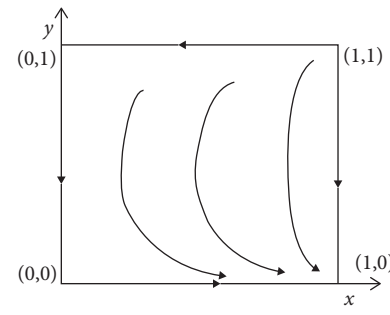

Figure 3: Replicated dynamic phase diagram of system 1 under condition (b).

3.2. Static Reward and Dynamic Punishment. Assume that the punishment strength of the local government is linearly related to the strategy choice of the enterprise; that is, $f(y) = (1 - y) \cdot \overline{f}$, where $\overline{f}$ indicates the upper limit of the punishment value, and the reward value is $\overline{w}$ constant. The evolutionary system in this case is named system 3. When the enterprise takes higher probability in the "Nonmanaged O_2" strategy, it will get more punishment from the local government. At this time, we can get five equilibrium points, namely, (0,0), (0,1), (1,1), (1,0), and (x_3, y_3); the point $(x_3, y_3) = (c_2/f + w + p_1 l_2 - (f - c_1 - p_1 l_1 + p_2(l_1 + l_3))/ - w - f + p_1 l_1 - p_2(l_1 + l_3))$.

In system 3, the $tr(J)$ of the points (0,0), (0,1), (1,1), and (1,0) cannot determine the sign and $de\ t(J)$ are minus signs. The $tr(J)$ of the points (x_3, y_3) is minus sign and $de\ t(J)$ is the plus sign. The characteristic roots of point (x_3, y_3) are a pair of characteristic complex roots, and the point is the stable focal point of system 3. Therefore, this evolutionary system has asymptotic stability, and point (x_3, y_3) is the stable focal point in this evolutionary system.

3.3. Dynamic Reward and Dynamic Punishment. Assume that the reward strength and the punishment strength of the local government are linearly related to the strategy choice of the enterprise, that is: $w(y) = y \cdot \overline{w}$, $f(y) = (1 - y) \cdot \overline{f}$. The evolutionary system in this case is named system 4. At this time, we can get five equilibrium points, namely, (0,0), (0,1), (1,1), (1,0), and (x_3, y_3); the point $(x_4, y_4) = (c_2/f + w + p_1 l_2 - (f - c_1 - p_1 l_1 + p_2(l_1 + l_3))/ - w - f + p_1 l_1 - p_2 (l_1 + l_3))$.

In system 4, the $tr(J)$ of the points (0,0), (0,1), (1,1), and (1,0) cannot determine the sign and $de\ t(J)$ are minus signs. The $tr(J)$ of the points (x_4, y_4) is minus sign and $de\ t(J)$ is the plus sign. Similarly, system 4 has asymptotic stability, and the point (x_4, y_4) is the focal point of stability in this evolving system.

4. Numerical Simulations

Based on the current stage of development and statistical data of Chinese smart cities, we propose a numerical study to simulate the behaviors of game subjects under different mechanisms, respectively, which can be theoretically applied to the problem of information security supervision in the construction of global smart cities.

4.1. Setting Initial Values. The application of the proposed evolutionary game model is demonstrated by taking the development of smart cities in China as an example. The initial input parameter data of the model are mainly obtained from industry analysis reports, national standards, and government websites of the central government and provinces and cities.

In recent years, with the accelerated development of a new generation of information technology, smart cities are developing rapidly in China. According to the Baidu City Brain White Paper, a total of 749 "smart city" pilot projects will be launched in China in 2021, and local governments at all levels have issued a total of 424 policy documents under the guidance of the central government to promote and regulate the construction of smart cities. By analyzing the text of 424 policy documents, we found that there were 162 policy documents that explicitly mentioned information security regulation and management rules, so we chose 0.4 as the initial value of x.

According to the 2021 Ernst & Young Global Information Security Survey released by Ernst & Young [45], about three-quarters of Chinese enterprises surveyed were unsure whether their cybersecurity defenses were adequate to deal with hackers' attacks, causing about one trillion yuan in losses. According to the "Research Report on the Information Security Status of Chinese Internet Users in 2021," the total amount of personal losses caused by information security incidents is about 20 billion yuan. According to the statistics of the weekly report on information security incidents released by the China National Internet Emergency Response Centre, there were about 120,000 information security incidents in the year 2021. According to "the 2019–2025 China Smart City Market Deep Panoramic Survey and 13th Five-Year Development Trend Forecast Report" statistics released by the China Research Institute of Industry, the number of enterprises in the smart city industry is expected to reach about 1,500 in 2021. In summary, we choose 0.25 as the initial value of y and set the social loss to 2, the loss caused to the local government to 8, and the loss caused to the enterprise itself to 50.

According to data from China and provincial, municipal, and district government procurement networks, nearly 4,300 bids were awarded for various types of smart cities in 2021, with a total award amount of about 108.5 billion yuan and an average investment of about 2.5 million yuan per project. In 2021, the Ministry of Industry and Information Technology issued the "Three-Year Action Plan for the High-Quality Development of Network Security Industry (2021–2023)," which shows that the investment in network security in telecommunications and other key industries accounts for 10% of the investment in information technology, while the "Information Security Technology Information Security Assurance Guide for Smart City Construction" clearly stipulates that the investment in information security should account for 8%–15% of the total project investment. Therefore, we set the management cost that enterprises need to invest when strengthening management to 6.

China's central government has a subsidy policy for enterprises involved in smart city operations, which is implemented by all local government. For example, Hefei City promulgated "Hefei City to promote the high-quality economic development of a number of policies." "For the development of smart city application scene innovation project investment of 3 million yuan and above, a one-time subsidy of up to 1 million yuan will be given on the basis of 10% of the investment amount on a merit basis." Wuhan City proposed "the main body of the shortlisted smart city project construction, according to its actual investment of 30% to give a maximum of 2 million yuan of financial support." The comprehensive policy of each city shows that the degree of subsidy varies from 10% to 30%. Combined with the specific requirements of the information security input ratio, we set the reward given by the local government to enterprises when strengthening management at 2.

For smart city information security punishment, according to China's information security-related laws, "for organizations that do not fulfill their obligations to protect network security and refuse to correct or cause harm to network security and other consequences, they will be given a fine of more than five thousand to one million yuan." Based on the bad information security practices against Tianxia Smart City Technology Co. in December 2021, a total penalty of 1 million yuan was imposed. This is consistent with the punishment standard set by law, and we set the punishment that enterprises receive when they do not strengthen management at 10.

Since the replication dynamic equations do not involve the returns of local governments and enterprises, they are not assigned here. Other values are set according to the model constraints, as shown in Table 4.

4.2. Simulation Results and Discussion. MATLAB R2019a software was used for evolutionary game model simulation. Three scenarios were constructed to investigate how enterprises respond to different government policies. Scenario 1 evaluates the behavioral strategy changes of game players under static reward and punishment mechanisms. Scenario 2 compares the strategies chosen by players under three dynamic mechanisms. Scenario 3 analyzes the impact of changes in the upper bounds of each parameter on the game subjects under the optimal reward and punishment mechanism.

4.2.1. Player Behavior of Evolutionary Games under Static Mechanisms. Figure 4(a) shows the change in the behavioral strategy of the enterprise under the static reward and punishment mechanism with different initial values of the local government. In this figure, the initial value of the local government is $x = 0.4, 0.6, 0.8$, and the initial value of the enterprise is $y = 0.25$. Figure 4(b) shows the change in the behavioral strategy of the enterprise under the static reward and punishment mechanism with different initial values of the enterprise. In this figure, the initial value of the local government is $x = 0.4$, and the initial value of the enterprise is $y = 0.25, 0.5, 0.75$. In Figure 4, firstly, from the trend of fluctuations, the probability of the enterprise choosing the Manage strategy shows an up-and-down oscillation

Table 4: Initial values of the simulation.

Parameter	x	y	c_1	c_2	l_1	l_2	l_3	w	f	p_1	p_2
Value Unit	0.25	0.4	5 million	6 million	8 million	50 million	2 million	2 million	10 million	0.1	0.9

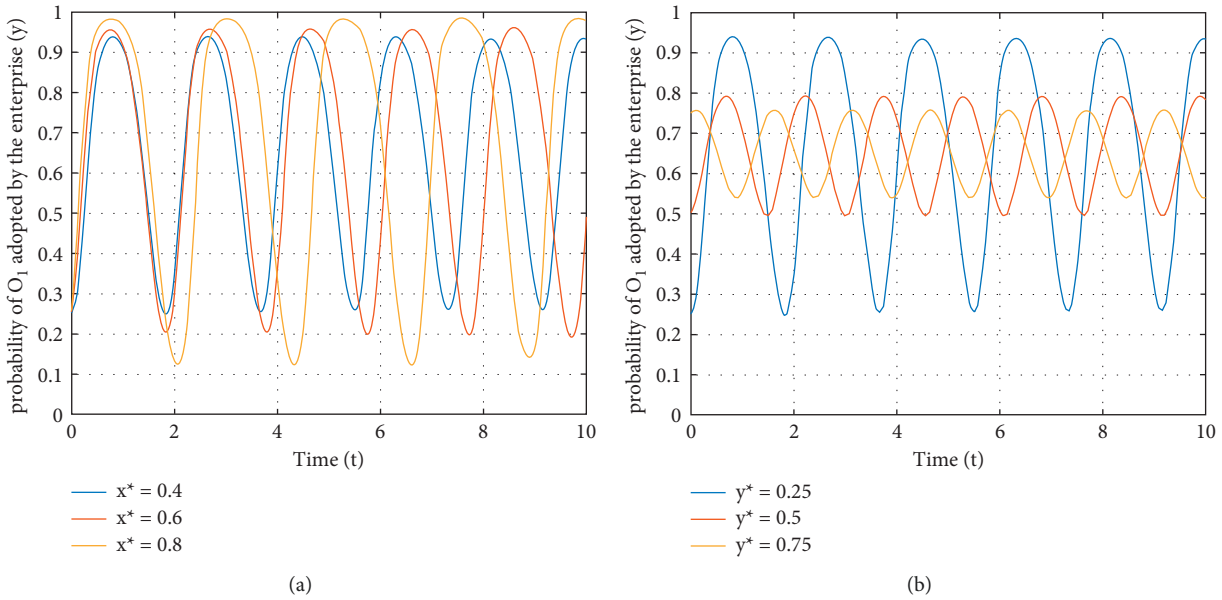

Figure 4: Evolutionary stabilization paths of local government and enterprise in system 1 for different initial values.

regardless of the initial values of local government and enterprise, and there is no stable point. Secondly, in terms of the frequency of volatility, as the probability of local government choosing the Supervise strategy becomes greater, the volatility cycle of enterprise is becoming larger. As the probability of enterprise choosing the Manage strategy becomes greater, the volatility cycle of the enterprise is becoming smaller. Finally, in terms of the magnitude of fluctuations, changes in the probability of local government choosing the Supervise strategy have a smaller magnitude of impact on enterprise, while changes in the probability of enterprise choosing the Manage strategy have a larger magnitude of impact on enterprise. From Figure 5, it can be seen that the evolution of the system is a periodic closed-loop curve around the center point (x*, y*) and there is no equilibrium point. The conclusion of the previous analysis is verified. In summary, the initial value is one of the decisive factors influencing enterprise's choice of the Manage strategy, and the change in the initial value of enterprise's choice of the Manage strategy has more influence on enterprise's behavioral strategy than the change in the initial value of local government's choice of the Supervise strategy.

4.2.2. Player Behavior of Evolutionary Games under Dynamic Mechanisms. Figure 6 shows the evolutionary paths of local government and enterprise under dynamic reward and static punishment mechanisms. Figure 7 shows a comparison of the evolutionary paths of local government and enterprise under static reward and dynamic punishment and dynamic

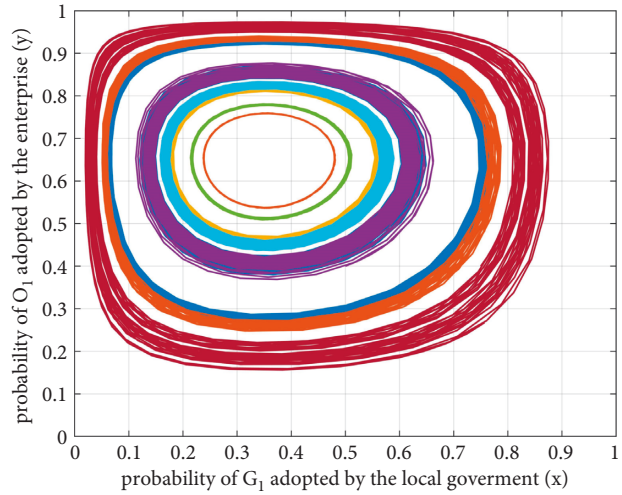

Figure 5: Dynamic evolutionary paths of local government and enterprise for system 1.

reward and dynamic punishment mechanisms. The initial value for the local government is still 0.4, and the initial value for the enterprise is still 0.25. From Figure 6, it is easy to see that the evolution of system 2 is a closed curve from the point (0.4,0.25), and there is no equilibrium point. From Figure 7, it can be seen that there are stabilization points for both system 3 and system 4. Both verify the conclusions of the previous analysis. The probability of local government adopting the Supervise strategy and enterprise adopting the

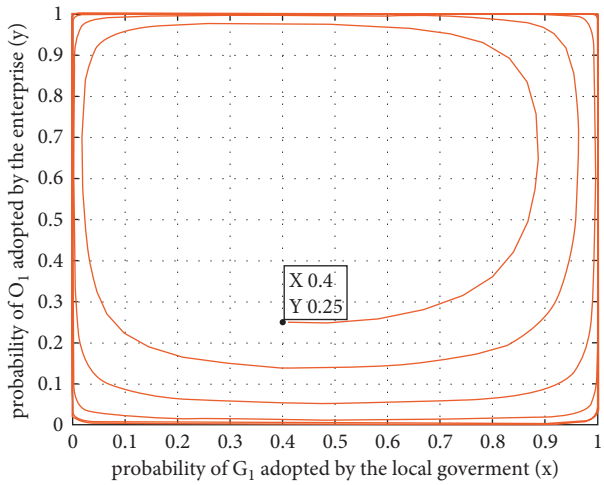

Figure 6: Dynamic evolutionary paths of local government and enterprise for system 2.

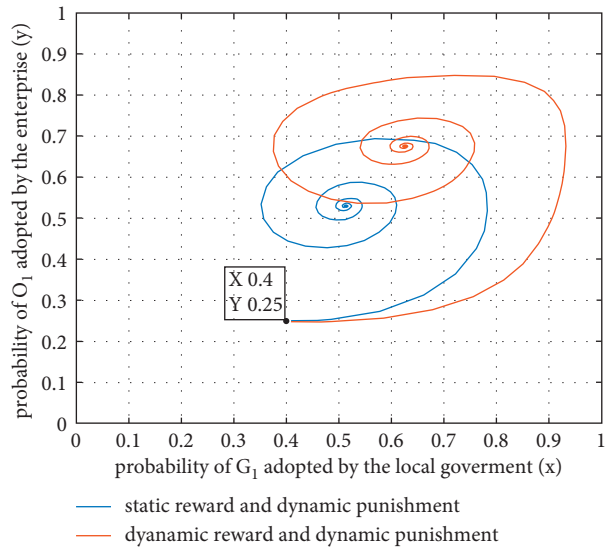

Figure 7: Comparison of the dynamic evolutionary paths of local government and enterprise for system 3 and system 4.

Manage strategy is higher, so the evolutionary equilibrium point of game subjects in system 4 is better. Therefore, dynamic reward and dynamic punishment is the optimal reward and punishment mechanism, followed by static reward and dynamic punishment, followed by dynamic reward and static punishment, and finally followed by static reward and static punishment.

Next, the paper will continue to discuss the evolutionary path of the upper limit changes of the key parameter values (c_1, c_2, w, and f) on the probability of strategy choice of local government and enterprise in system 4.

Under the optimal reward and punishment mechanism, the initial value of the local government is still 0.4, and the initial value of the enterprise is still 0.25. The simulation results are shown in the following.

Figure 8 shows the effect of the change in the upper bound of the supervisory cost (c_1) of local government on the behavioral strategies of local government and enterprise under the optimal reward and punishment mechanism. As can be seen from Figure 8, firstly, from the evolutionary direction, the probability of local government choosing the Supervise strategy and the probability of enterprise choosing the Manage strategy are both negatively related to the increase of the supervisory cost ceiling. Secondly, in terms of the degree of change, enterprise is more sensitive to the increase in the supervisory cost cap compared to local government. In addition, the evolutionary stability of both sides of the game tends to be 0 when the upper bound of c_1 rises to 19. This is because the original game equilibrium is disrupted. This verifies the conclusion of the previous analysis. Taken together, the increased cost of supervision does not promote well the adoption of aggressive strategies by both sides of the game with a higher probability.

Figure 9 shows the effect of the change in the upper bound of the supervisory cost (c_2) of local government on the behavioral strategies of local government and enterprise under the optimal reward and punishment mechanism. As can be seen from Figure 9, firstly, in terms of evolutionary direction, the probability of local government choosing the Supervise strategy is positively related to the increase in the upper limit of operating cost, and the probability of enterprise choosing the Manage strategy is negatively related to the increase in the upper limit of operating cost. Secondly, in terms of the degree of change, when c_2 changes from 6 to 10, the change in local government is larger, while the change in enterprise is minimal. This may be because an increase in operating cost within a certain range does not affect the change in enterprise's decision-making behavior, and once a certain threshold is exceeded, enterprise's sensitivity to operating cost will increase rapidly. The high investment in operating cost makes the enterprise biased to adopt the Manage strategy with a lower probability. When c_2 changes to 16, the evolution of the local government stabilizes towards 1, and the evolution of the enterprise stabilizes towards 0. This verifies the conclusions of the previous analysis.

Figure 10 shows the effect of the change in the upper bound of the reward (w) of local government on the behavioral strategies of local government and enterprise under the optimal reward and punishment mechanism. As can be seen from Figure 10, firstly, from the evolutionary direction, the probability of local government choosing the Supervise strategy and the probability of enterprise choosing the Manage strategy are both negatively related to the increase of the reward ceiling. Secondly, in terms of the magnitude of change, when w changes from 2 to 6, the change is greater for local government compared to enterprise. When w changes to 12, the strategies of both sides of the game show an up-and-down oscillation, and the oscillation is increasing in magnitude and period. It can be seen that the adoption of appropriate incentive subsidies at the initial stage is conducive to promoting enterprise to increase investment in information security management and avoid information security incidents. However, in the long run, high subsidies tend to be counterproductive. A possible explanation is that subsidy incentives increase the financial burden on local

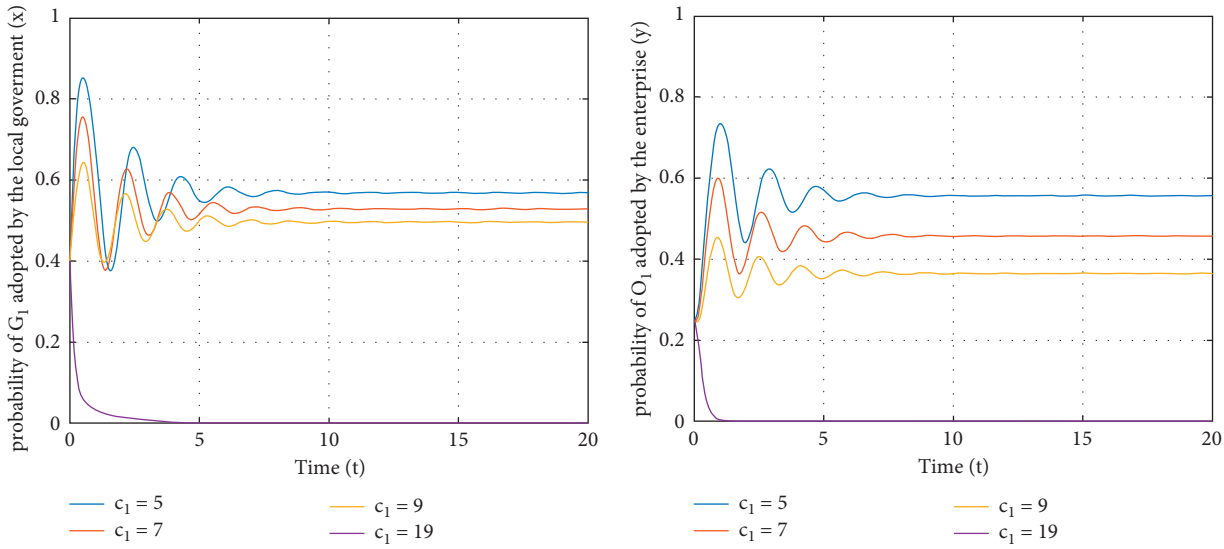

Figure 8: The impact of raising the upper limit of c_1 on local government and enterprise.

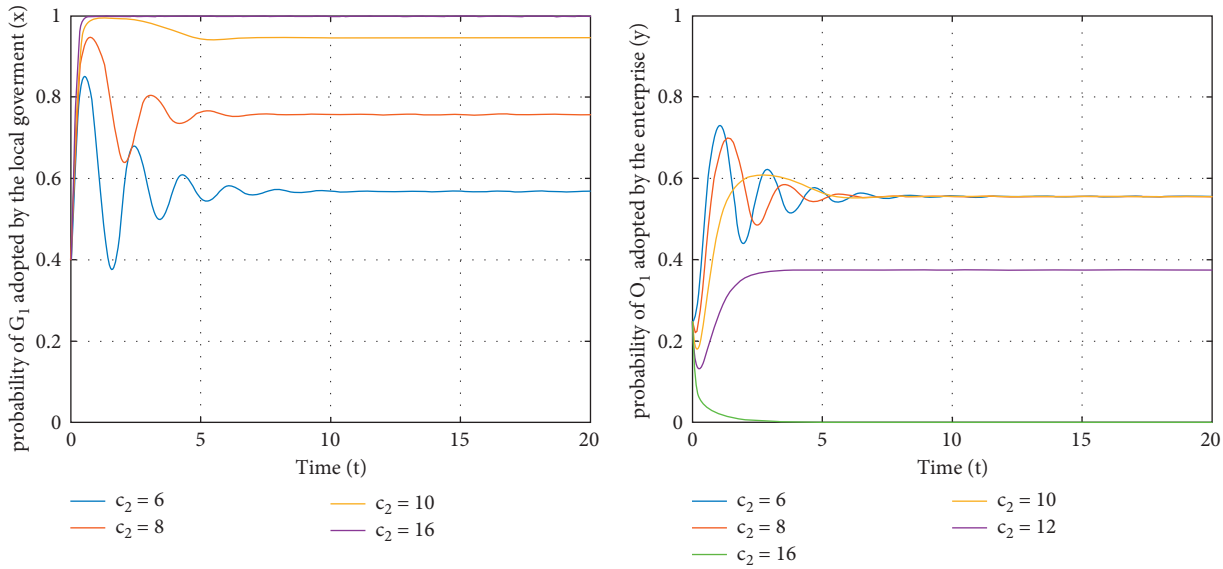

Figure 9: The impact of raising the upper limit of c_2 on local government and enterprise.

government, which are thus biased towards the Non-supervise strategy. At the same time, in the case of information asymmetry, there is a possibility that enterprise may use the incentive subsidy for other management aspects to gain revenue, resulting in the lapse of the subsidy. This phenomenon has been verified in many industries.

Figure 11 shows the effect of the change in the upper bound of the punishment (f) of local government on the behavioral strategies of local government and enterprise under the optimal reward and punishment mechanism. As can be seen from Figure 10, in terms of evolutionary direction, the probability of local government choosing the Supervise strategy is negatively related to the increase in the upper limit of punishment, and the probability of enterprise choosing the Manage strategy is positively related to the increase in the upper limit of punishment. This suggests that the increase in local government punishment will lead to an increase in the probability of enterprise adopting the Manage strategy, making the probability of information security risk events lower and thus the probability of local government supervision lower.

4.3. Analysis of Results. The simulation results show that there is no stable equilibrium point in the system under the static reward and punishment mechanism, and there is no condition that makes the enterprise choose the Manage strategy if the initial conditions are changed. Under the dynamic reward and punishment mechanism, there is no stable equilibrium point in the system under the dynamic reward and static punishment mechanism, there is a stable equilibrium point in the system under both the static reward

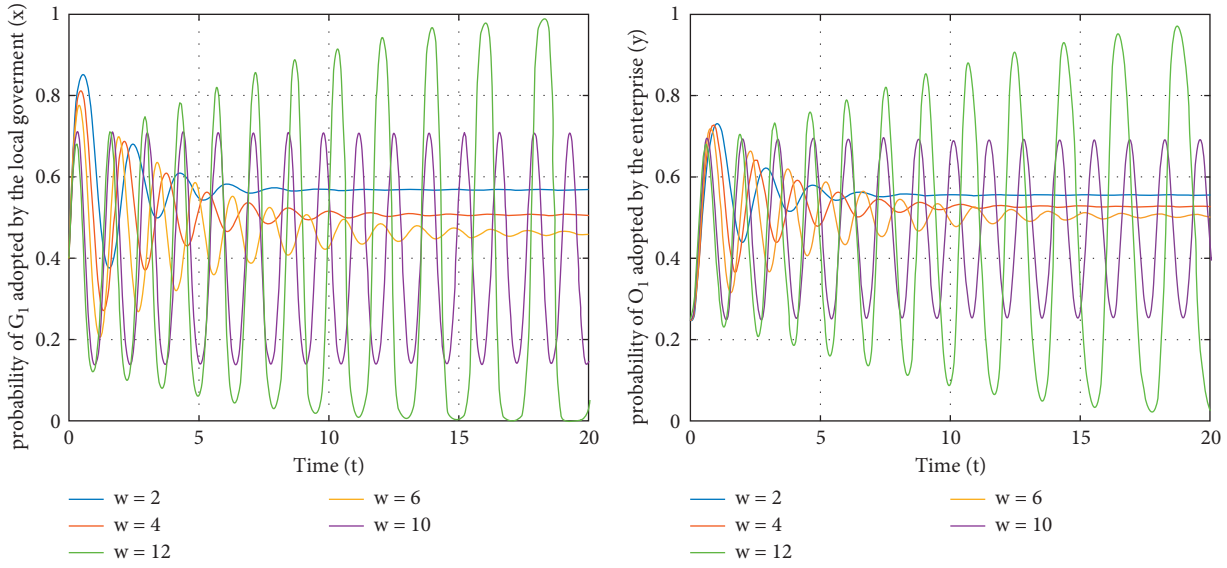

Figure 10: The impact of raising the upper limit of w on local government and enterprise.

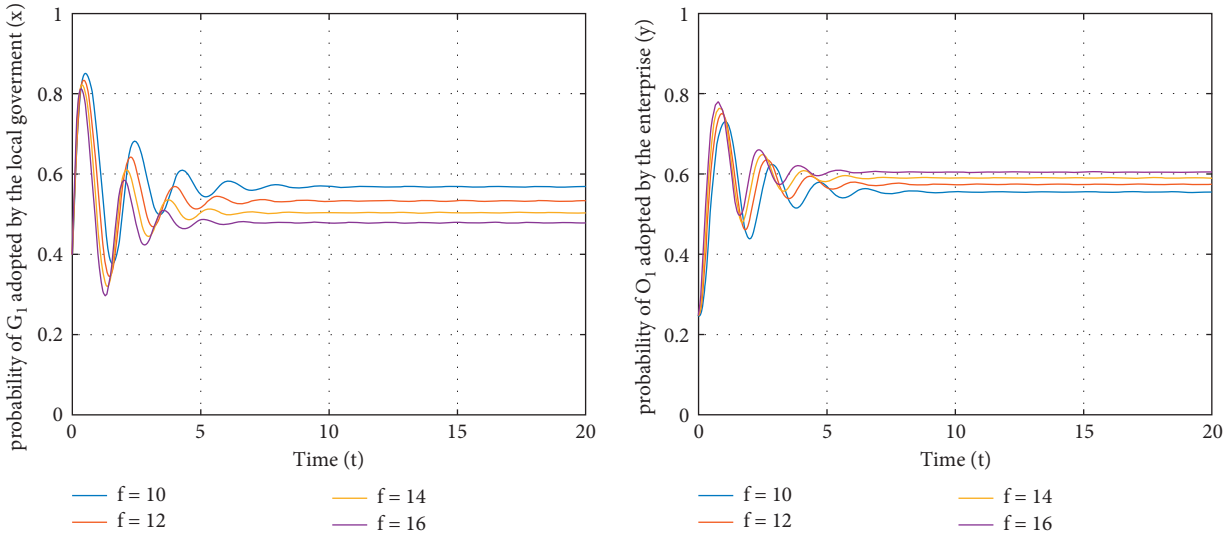

Figure 11: The impact of raising the upper limit of f on local government and enterprise.

and dynamic punishment and dynamic reward and dynamic punishment mechanisms, and the latter is the more optimal mechanism. Under the optimal reward and punishment mechanism, the probability of the local government choosing the Supervise strategy is negatively related to the increase of supervision cost and the upper limit of reward and punishment and positively related to the increase of management cost. The probability that enterprise chooses the Manage strategy is negatively correlated with the increase of supervision cost, management cost, and upper limit of reward and positively correlated with the increase of the upper limit of punishment.

Combined with the simulation results, this paper puts forward some suggestions for the information security supervision of smart cities. Local government reward and punishment play a key role in stimulating smart city enterprise to adopt enhanced information security management, but a scientific policy of reward and punishment needs to be implemented. The improvement of the information security supervisory system for smart cities often lags behind market development, which leaves many incentives to be enforced by traditional regulators based on old regulatory norms. Obviously, this lacks dynamism and timeliness. As we have studied, in the process of information security supervision in smart cities, dynamic reward and dynamic punishment mechanisms provide more incentives for local government and enterprise, and both increase the probability of both sides of the game to adopt positive strategies, so local government should adopt dynamic reward and dynamic punishment mechanisms when implementing supervision on enterprise. In terms of reward, ongoing subsidy incentives can place a huge financial burden

on the government. For enterprise, it is also not the case that higher incentives are better. Excessive incentive subsidies can sometimes be counterproductive, so be flexible and change in the actual supervisory process. For example, start-ups have financial and technological constraints [41] and can be poorly run in subsequent operations once the initial subsidy expires [46]. At this point, local government needs to focus on reward. Growing and mature enterprise is stronger on its own and has a certain degree of risk resistance. At this time, the local government needs to reduce the incentive subsidies to punishment. In terms of punishment, too low punishment has a little restraining effect on enterprises, so the punishment should be increased for enterprises that do not strengthen information security management, and at the same time, recovery measures should be taken and punishment imposed on enterprises that have received subsidies. Larger punishment can have a high probability of deterrence and promote enterprise to adopt a higher probability of strengthening information security management strategy, indirectly relieving the supervisory pressure of the local government and reducing supervisory costs.

5. Conclusion

Strengthening information security supervision can effectively promote the healthy development of smart cities. Local governments, smart city enterprises, and academia are currently studying the issue of government incentives for relevant enterprises. Most previous studies have explored the effectiveness of incentives from a qualitative perspective and have not been able to reveal the dynamics of the strategic choices of local governments and enterprises on information security issues under different policies. Therefore, this paper establishes an evolutionary game model for local governments and smart city enterprises, analyzes the equilibrium point of each system and its stability under different reward and punishment mechanisms with the help of case data from China, and explores the impact of increasing the upper limit value of key parameters on the evolutionary stability strategy of game subjects under the optimal mechanism. The results are as follows: First, the initial value is one of the decisive factors influencing the choice of management strategy of the enterprise. Second, by comparing the four reward and punishment mechanisms, we found that the dynamic reward and dynamic punishment mechanism is the optimal mechanism. Finally, we analyze the effect of increasing the upper bound of key parameters on the strategy choice of both sides of the game under the optimal mechanism. Among them, increasing punishment can effectively promote both sides of the game to adopt active strategies, and reasonably adjusting the reward policy can also mobilize the information security behavior of enterprises.

At the theoretical level, this paper explores the applicability of evolutionary game theory to the problem of information security supervision in smart cities, providing a new perspective for the current research in related fields. At the practical level, this paper finds the optimal mechanism for information security supervision of smart city by constructing game models under different reward and punishment mechanisms and puts forward feasible optimization suggestions, which provides some reference for the practical regulation of information security of smart city. At the same time, there are still shortcomings in this paper. Firstly, in the dynamic reward and punishment mechanism, the strategy choice of the game subject does not necessarily show a linear relationship with the upper limit of the reward and punishment but may be a nonlinear relationship. Secondly, in the process of information security supervision of smart city, in addition to the two sides in the paper, it will also involve the influence of the decision-making behavior of higher-level government, the public, and other subjects. Finally, there may be organizations or individuals with different degrees of influence within the game group, and there may be some complex environments outside, which remains to be explored whether this will affect the evolutionary stability strategy of the whole group. More in-depth research will be conducted on the basis of the above in the future.

Data Availability

The data used to support the findings of this study are included within the paper.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors acknowledge the National Social Science Foundation of China for supporting this research. This research was supported by the National Social Science Fund of China (no. 18BTQ055).

References

[1] F. Victoria, M. F. Jose, and G. Rudolf, "Smart City implementation and discourses: an integrated conceptual model. The case of Vienna," *Cities*, vol. 78, pp. 4–16, 2018.

[2] E. Ismagilova, L. Hughes, Y. K. Dwivedi, and K. R. Raman, "Smart cities: advances in research—an information systems perspective," *International Journal of Information Management*, vol. 47, pp. 88–100, 2019.

[3] P. Singh, Y. K. Dwivedi, K. S. Kahlon, R. S. Sawhney, A. A. Alalwan, and N. P. Rana, "Smart monitoring and controlling of government policies using social media and cloud computing," *Information Systems Frontiers*, vol. 22, no. 2, pp. 315–337, 2020.

[4] S. Kehua, L. Jie, and F. Hongbo, "Smart City and the Applications," in *Proceedings of the 2011 International Conference on Electronics Communications and Control (ICECC)*, pp. 1028–1031, IEEE, Ningbo, China, September 2011.

[5] C. Aandres and A. Enrique, "Smart City and information technology," *A review Cities*, vol. 93, pp. 84–94, 2019.

[6] Z. Allam and P. Newman, "Redefining the smart city: culture, metabolism and governance," *Smart Cities*, vol. 1, no. 1, pp. 4–25, 2018.

[7] S. Liyin, H. Zhenhua, W. Siuwai, S Liao, and Y Lou, "A holistic evaluation of smart city performance in the context of China," *Journal of Cleaner Production*, vol. 200, no. 1, pp. 667–679, 2018.

[8] B. S. Elias and K. John, "On the social shaping dimensions of smart sustainable cities: a study in science, technology, and society," *Sustainable Cities and Society*, vol. 29, pp. 219–246, 2017.

[9] P. Guido and R. Mariangela, "A taxonomic analysis of smart city projects in North America and Europe," *Sustainability*, vol. 18, no. 12, p. 7813, 2020.

[10] K. Milan, S. Dominika, and V. Josef, "Comparison of smart city standards, implementation and cluster models of cities in North America and Europe," *Sustainability*, vol. 13, no. 6, p. 3120, 2021.

[11] Y. Jeyun, K. Youngsang, and K. Daehwan, "Regional smart city development focus: the South Korean national strategic smart city program," *IEEE Access*, vol. 9, pp. 7193–7210, 2020.

[12] Z. Kuan, N. Jianbing, and Y. Kan, "Security and privacy in smart city applications: challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[13] Z. Yanxia, "A study on the balance between government information disclosure and personal information protection in epidemic prevention and control," *Journal of Hubei Police College*, vol. 33, no. 2, pp. 25–33, 2020.

[14] C. Lim, G. H. Cho, and J. Kim, "Understanding the linkages of smart-city technologies and applications: key lessons from a text mining approach and a call for future research," *Technological Forecasting and Social Change*, vol. 170, Article ID 120893, 2021.

[15] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: literature review and development of a smart city interaction framework," *Information Systems Frontiers*, pp. 1–22, 2020.

[16] Z. Jing, "Problems of Internet security and countermeasures: a perspective on the "prism gate" incident," *Journal of Jiangxi Police Academy*, vol. 4, pp. 66–69, 2014.

[17] M. Chen, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Reports*, vol. 7, pp. 7999–8012, 2021.

[18] M. Masike, M. Annlize, and V. S. Sune, "Validation of a socio-technical management process for optimising cybersecurity practices," *Computers & Security*, vol. 95, Article ID 101846, 2020.

[19] Q. K. J. Su, *Computer Crime and Security Survey*, pp. 1–18, Goverment Technology, New Zealand, 2010.

[20] S. Sengan, S. V, I. V, P. Velayutham, and L. Ravi, "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning," *Computers & Electrical Engineering*, vol. 93, p. 107211, 2021.

[21] Z. Kai, G. Yihang, X. Shang, and W. Zhen, "Research on the construction of information security guarantee system for smart cities under big data environment," *Knowledge Management Forum*, vol. 6, no. 6, pp. 364–374, 2021.

[22] N. Repal and T. Jamasb, "Incentive regulation and utility benchmarking for electricity network security," *Economic Analysis and Policy*, vol. 48, pp. 117–127, 2015.

[23] J. Luning, "Positive and Negative Incentives for Information Security Policies," *China Information Security*, vol. 8, p. 110, 2014.

[24] L. Can, Z. Yongjie, and H. Sheng, "The optimization of the legal system for the cybersecurity governance of smart cities in China," *Korean-Chinese Social Science Studies*, vol. 19, no. 4, pp. 312–331, 2021.

[25] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, 2009.

[26] Y. Yang, "On the regulatory structure of the risk of personal biometric information application," *Administrative Law Studies*, vol. 6, pp. 101–114, 2021.

[27] J. M. Smith and G. R. Price, "The logic of animal conflict," *Nature*, vol. 246, no. 5427, pp. 15–18, 1973.

[28] J. M. Smith, "The theory of games and the evolution of animal conflicts," *Journal of Theoretical Biology*, vol. 47, no. 1, pp. 209–221, 1974.

[29] K. Po, H. Ying, and S. Junguo, "A study of local government environmental control behavior in the context of central environmental protection inspectors," *Operations Management*, vol. 30, no. 10, pp. 27–133, 2021.

[30] Y. Zhihua and T. Xijin, "Humanistic analysis of drug quality and safety regulation based on evolutionary game," *Management Comments*, vol. 33, no. 5, pp. 64–75, 2021.

[31] Z. Xiaofeng, H. Xiaoting, and B. Gaofeng, "Research on the quality control of micro-government information disclosure considering reputation," *Library Theory and Practice*, vol. 5, pp. 70–76, 2019.

[32] R. Mahmoudi and M. Rasti-Barzoki, "Sustainable supply chains under government intervention with a real-world case study: an evolutionary game theoretic approach," *Computers & Industrial Engineering*, vol. 116, pp. 130–143, 2018.

[33] L. Xingwei, H. Ruonan, D. Jiachi, J Li, and Q Shen, "Research on the evolutionary game of construction and demolition waste (CDW) recycling units' green behavior, considering remanufacturing capability," *International Journal of Environmental Research and Public Health*, vol. 18, no. 17, p. 9268, 2021.

[34] L. Hongyu, L. Hongyong, L. Xingwei, and C. Longjun, "An evolutionary game theory study for construction and demolition waste recycling considering green development performance under the Chinese government's reward–penalty mechanism," *International Journal of Environmental Research and Public Health*, vol. 17, no. 17, p. 6303, 2020.

[35] L. Cong, H. Weilai, and Y. Chao, "The evolutionary dynamics of China's electric vehicle industry–Taxes vs. Subsidies," *Computers & Industrial Engineering*, vol. 113, pp. 103–122, 2017.

[36] Z. Min and Q. Peng, "Evolutionary game study on the protection and use of personal data of over-collected APPs under government regulation," *Intelligence Exploration*, vol. 11, pp. 8–18, 2020.

[37] Q. Xinchi and H. Guisheng, "Research on information security governance of platform based on three-party evolutionary game," *Modern Intelligence*, vol. 40, no. 7, pp. 114–125, 2020.

[38] Z. Kai, W. Zhen, C. Dan, and Z. Dongdong, "Evolutionary game analysis of information security regulation strategy in smart cities," *Modern Intelligence*, vol. 41, no. 3, pp. 3–14, 2021.

[39] V. Morta, H. Ying, B. Thomas, and J. Helge, "Smart cities and cyber security: are we there yet? A comparative study on the role of standards, third party risk management and security ownership," *Computers & Security*, vol. 83, pp. 313–331, 2019.

[40] Z. Hui and G. Dandan, "U.S. Network Geographic Information Security Regulation and Its Implications for China," *Theoretical Discussion*, vol. 4, pp. 139–143, 2015.

[41] W. Huawei, S. Xiaomin, and Z. Lijian, "Research on fiscal policies to promote the construction of smart cities," *Business Economy*, vol. 3, no. 3, 2021.

[42] Z. Chang, X. Xiaolin, W. Junze, and Z. Congcong, "Analysis of non-traditional security in information sharing and use in smart cities: the case of," *New Online Political Advertising*, E-Government, vol. 7, pp. 9–19, 2018.

[43] Inflated Revenue of More than 3 Billion, Tianxia Intelligence and 23 Related Personnel Received Fines," https://cj.sina.com.cn/articles/view/1704103183/65928d0f02002m7yb.

[44] C. Zhuolun, "Application of Environmental Ecological Strategy in Smart City Space Architecture Planning," *Environmental Technology & Innovation*, vol. 23, Article ID 101684, 2021.

[45] E. Ernst and Y. Young, "Releases the 2021 Ernst & Young Global Information Security Survey," 2021, https://www.yicai.com/news/101178234.html.

[46] I. M. F. Oomens and B. M. Sadowski, "The importance of internal alignment in smart city initiatives: an ecosystem approach," *Telecommunications Policy*, vol. 43, no. 6, pp. 485–500, 2019.