Hindawi
Complexity
Volume 2024, Article ID 8849477, 17 pages
https://doi.org/10.1155/2024/8849477

Research Article

Analysis of Digital Security Governance under the Objectives of Digital Ecology: A Three-Party Evolutionary Game Approach

Zhen Tian [1] **Chuchu Jiang** [1] **and Gangyi Yue** [2]

[1] *College of Economics and Management, Zhengzhou University of Light Industry, Zhengzhou 450001, China*
[2] *School of Business Administration, Zhengzhou University of Science and Technology, Zhengzhou 450001, China*

Correspondence should be addressed to Chuchu Jiang; chuu313@163.com

Received 24 June 2023; Revised 19 March 2024; Accepted 1 April 2024; Published 16 April 2024

Academic Editor: Chittaranjan Hens

With the rapid development of the digital economy, there has been an explosion in the amount of data generated. Data have become a vital resource for nations, just as tangible assets and human capital are crucial factors of production. Consequently, protecting digital security has become paramount. However, the increasing frequency of various data security incidents in recent years has exposed issues such as inadequate platform governance, lack of government regulation, and incomplete digital security governance (DSG) mechanisms. This study aims to create a healthy and open digital ecosystem and proposes a new digital security governance framework. It subdivides traditional government departments into local governments and the central government. Together with third-party platforms, they are analyzed as participants in an evolutionary game. The study examines the evolutionary stability of strategy choices made by each party and explores the relationship between key factors such as negative externalities, data security incident probabilities, and their impacts on strategy selection using numerical simulations. The research findings indicate the following. (1) Key parameters such as implicit benefits, government subsidies, and negative externalities play a significantly positive role in the development of the digital ecosystem. (2) The central government consistently tends towards emergency response, considering the overall societal perspective, as long as it is capable of bearing the costs. (3) Local governments may exhibit free-riding behavior during the governance process. To address this, it is important to increase the willingness of third-party platforms to govern and oversee the participation of local governments, which is an effective way to prevent data crises. The study also identifies different governance models in various environments: (1) a digital security governance model in a stable market environment, involving increased central government intervention and supervision of local governments' participation; and (2) a digital security governance model in the event of a data crisis, where the central government establishes subsidies that exceed the governance costs of local governments to enhance the willingness of third-party platforms to govern. Finally, recommendations and strategies are presented to enhance the level of digital security governance.

1. Introduction

Digital ecology has become an important means for social progress and economic prosperity and thus is an important pillar in the construction of Digital China [1]. China's digital ecological construction is on the ascendant, as a large amount of data came into being, and the problem of data insecurity followed. For example, the employees of Ping An Life Insurance Company Limited illegally sold 40,000 pieces of customer information, and Super Star Learning Link software leaked over 170 million pieces of private data, damaging personal information. Unbridled data collection, excessive data mining and misuse, and cyberattacks have become increasingly commonplace [2]. Platform enterprises characterized by digital drive and network collaboration have commonly deposited huge amounts of data during development, and problems such as data monopoly, data security, and personal information protection have emerged [3]. If digital security governance (DSG) is not strengthened, data and information can be arbitrarily collected, tampered with, trafficked, and disseminated, severely undermining the national and public interests. DSG is the key to improving the security level of contemporary organizations [4, 5] as it embeds security into the organizational structure and all relevant business dimensions and factors across the organization, helping to capture strategic objectives and appropriately manage security risks [5]. Implementing DSG and establishing strong safeguards and dynamic and constant security protection mechanisms enable the proper protection and secure use of sensitive data. This strategy allows for continuous security and protection of organizational assets [6, 7].

However, due to the late start of DSG in China [8], there are still issues concerning data security measures, interdepartmental collaboration, digital infrastructure development, industry regulation, and digital national sovereignty [8]. Although a preliminary institutional framework for DSG has been formed, regulating behaviors directly on various platforms is still challenging, and the government mainly requires them to abide by their obligations rather than exercising its regulatory duties [9]. Escalating user concerns about privacy and data security has posed new challenges to DSG, and therefore, continuously updated research is needed to adapt to these changes. Meanwhile, the DSG literature is primarily descriptive, focusing on normative standards, generic frameworks, and the individual level [10, 11] while ignoring the complexity of the interactions between different subjects. It should be noted that DSG is not an endeavor that can be carried out by one party alone, and multiple governance roles, responsibilities, and strategies are key pillars in developing robust governance and security processes and procedures [12, 13]. However, current studies investigate the game between platforms and local governments [14, 15]. However, as the highest level of responsibility for data security, the central government has not been considered yet. It is important as the central government plays a key role in DSG, and its responsibilities include regulation-making, regulatory enforcement, and policy formulation. Introducing central government into the tripartite evolutionary game can strengthen the risk management capabilities of digital security governance systems. First and foremost, this expansion facilitates a more comprehensive consideration of interests. Local governments and central governments represent distinct sets of stakeholders with diverse priorities and concerns. Local governments emphasize regional development, while central governments focus on national security, strategic imperatives, and citizen welfare. By incorporating these various perspectives, the dynamics of the game become enriched, allowing for a more nuanced understanding of the competing interests at play. Moreover, this expansion clarifies the delineation of responsibilities and promotes orderly coordination among stakeholders. By defining the roles and responsibilities of platforms, local governments, and central governments in digital security governance, stakeholders can minimize confusion, duplication of efforts, and jurisdictional conflicts. Clear lines of accountability facilitate effective decision making, streamline operational processes, and enhance the overall efficiency and effectiveness of governance mechanisms. Therefore, it is necessary to conduct an in-depth study of DSG while considering digital ecology and from the perspective of game theory and centered on data security, with the participation of third-party platforms, local governments, and the central government.

This paper constructs a cross-industry and cross-domain DSG model and a more comprehensive, integrated, and flexible conceptual framework that reveals the DSG mechanism in digital ecology. This study contributes to the construction of a theoretical system of DSG and provides an in-depth understanding of the roles, relationships, and responsibilities of governments, enterprises, and individuals in data security. In addition, this study helps to predict future development trends, formulate corresponding governance strategies in advance, and assist decision makers in better understanding the problems, predicting risks, and formulating specific and effective policies, regulations, and data security strategies. Nevertheless, a continuous feedback mechanism between theory and application is required to better respond to the ever-changing data security challenges.

2. Literature Review

2.1. DSG Study. “DSG” was first proposed by Gartner, who claimed that DSG is a complete chain from the decision-making level to the technical level, from the management system to the tool support, and runs through the whole organizational structure from top to bottom [16]. Some scholars have expanded on this connotation, arguing that strategic security considerations in the digital environment are called DSG [5, 10, 11, 17]. Furthermore, they aimed to maintain the confidentiality, integrity, and availability of data assets [16], achieving the goals and the proper management of security risks [5, 18] in response to the increasing number of cyberattacks [6]. Although different scholars have different definitions of “DSG,” the core is to coordinate the rights and interests of the various stakeholders and protect the entire data life security cycle. Throughout the data security legislation and governance practices of countries worldwide, the DSG model has roughly passed through three stages, from responsive governance focusing on guidance and regulation to centralized governance with institutional and mandatory, and then to agile governance with the participation of multiple governance subjects and the flexible use of a variety of governance tools [12]. In the current stage of multiple governance, the three-party evolution game is an effective model for studying game relationships between various subjects.

Previous works have always paid attention to DSG. On the one hand, the widespread use of digital technologies has provided new opportunities and challenges for various industries. Indeed, some researchers have explored the transformative impact of DSG on various aspects of public health [19], higher education [20], government information assets [21], and supply chain finance [22, 23], which can enhance their risk management capabilities, protect privacy, and promote open information sharing and service improvement. On the other hand, some works have conducted theoretical or empirical studies from the subdivisions of DSG regarding cross-border data flow supervision [24], personal privacy protection [25], and data opening and sharing. For example, Li et al. [26] built a binary network model and an associated network to identify the risk of the cross-border flow of important data and provided a quantitative method for early warning management for cross-border data. However, the DSG literature is primarily descriptive, focusing mostly on prescriptive standards and generic frameworks [10, 11] or analyzing problems using the DSG process, such as inadequate data privacy protection and legal security systems [27]. Specifically, current works lack a holistic, top-down analysis of the DSG system. Although there are strong interconnections between these areas, both cross-border and open sharing of data involve privacy protection issues, and a healthy and effective DSG framework needs to balance these aspects to ensure the secure data flow and protection of individual privacy while simultaneously facilitating the openness and data sharing to promote innovation and sustainable development in society.

2.2. Platform DSG Research. Third-party platforms often collect and process large amounts of personal data as a constituent feature of their business model [28]. There are many studies on data security in platform companies, mainly based on the profit-seeking nature of the platforms. Data misuse and public opinion dissemination can be divided into two main categories. The former manifests itself in the excessive collection of user data by platforms [29, 30], the implementation of big data price discrimination [31], and the unauthorized use of information [32]. The latter manifests in disseminating false information by platforms [33, 34] and manipulating public opinion [7, 35]. For example, Hou et al. [14] argued that there is an information inequality between platforms and individuals, and Yao [3] analyzed the “big data-based price discrimination” by constructing a game model among consumers, platform enterprises, and the government. They started with the misuse of data by platforms and examined the regulatory mechanisms among users, platforms, and governments.

However, third-party platforms allow any account to register and log freely and express their views, which has resulted in a large and generally low-quality data of the online information ecosystem. At the same time, users can influence the dissemination and use of information through retweeting, liking, and commenting. Thus, third-party platforms act as a medium or tool carrier in their own right rather than subjective actors. For example, some users send spam through Weibo [36], and in Brazil, WhatsApp has been used for virtual kidnapping and fraudulent extortion [37].

2.3. Summary. The literature presented above highlights that current research on DSG mainly focuses on the theoretical level. Specifically, these studies focus on a specific area of the DSG challenges, exploring its current situation, problems, and optimization paths. In addition, most scholars have focused on the active behavior of third-party platforms when studying the formation of data hazards, while relatively little consideration has been given to the factor of their passively becoming a channel of abuse. Similarly, the central government’s role in the DSG process has been somewhat neglected. Given this situation, this paper explores DSG from the perspectives of various stakeholders, such as policy promulgation, call for response, and implementation, to build an evolutionary game model of the central government, local governments, and third-party platforms, analyze their possible behavioral strategies, and make the corresponding suggestions.

3. Construction of the Evolutionary Game Model

3.1. Theoretical Framework

3.1.1. The Subject of DSG. The proposed DSG is a comprehensive management strategy involving multiple actors that protects and maintains data confidentiality, integrity, and availability. In DSG, the central government has the overall coordination and regulatory responsibilities at the national level, and local governments and third-party platforms take measures to fulfill their governance obligations jointly.

The central government is the leader and policy maker of the DSG process. It is responsible for coordinating major national data security matters and important work, establishing a national data security coordination mechanism, supervising and managing the data security policies and regulations of various departments, institutions, and organizations, and protecting the basic rights and interests of individuals and organizations in terms of data security. Various localities and enterprises may have different interests and governance standards, requiring the central government to act as a coordinator and establish nationwide consistent standards and norms to ensure consistent and controllable data security. DSG by all parties cannot spontaneously reach a state of equilibrium, and the involvement of the central government in supervision and management is an important factor in promoting active action by platforms and local governments. Furthermore, the central government possesses broader resources and power, allowing for the swift allocation of necessary technological, financial, and human resources when data security incidents occur. Particularly in responding to large-scale or severe data security events, a significant amount of resources and cross-departmental coordination are required, which local governments may struggle to handle independently. For example, the central government can rely on national-level security agencies and expert teams to quickly diagnose issues, assess risks, and formulate effective response measures. Therefore, within the overall national context, the central government assumes the ultimate role in emergency response.

Local governments are facilitators and important participants in the DSG process and belong to “dispatched agencies” of the central government. Local governments have the responsibility to assume the responsibility of DSG within their duties and formulate data security behavior norms and group standards according to the law. They should conduct self-examination and cooperate with third-party platforms to ensure the development and utilization of data and industrial development in the region with data security. The central government supervises local governments and undertakes the obligation to reduce illegal data acquisition and utilization.

Third-party platforms are the executors and policy implementers of the DSG process, with data analysis as the main business or data as a production factor [15], providing fast information aggregation and circulation channels. As an important carrier of data flow, the platforms must handle a large amount of data, including user-generated data, server logs, and application data. These data are the basis for the platforms' operation and the key to its services and functions. Platforms can analyze data to discover user behavior patterns, understand user needs, optimize services, and attract more users to gain revenue. This requires the platforms to take appropriate technical and management measures to ensure the security of the data in the process of use and to avoid eavesdropping, tampering, and interception.

3.1.2. Analysis of the Subject Benefits. As a data aggregation and diffusion center, the platforms can set up access control mechanisms [25] using keywords [38] to block, delete [39], or restrict the flow of sensitive or offending content. Local governments give platforms the responsibility as market regulators to monitor the quality, combat infringement, and control prices [9]. Note that local governments can become platforms' users to discover, search, and review illegal information on the platforms. Besides, the central government provides policy support and guidance to local governments or platforms and can issue bans or penalties to local governments or platforms based on data breaches. In regulating the implementation of a data security regime, the central government represents the public's interests, emphasizing how to maximize society's overall interest and general welfare. In contrast, local governments mainly consider the interests of local authorities, and platforms are essentially profit-making organizations, which may deviate from the central government's interests and form a bargaining game. Hence, promoting the cooperation between local governments and third-party platforms, where the two jointly review the content of Internet information from different aspects, can compensate for the deficiencies in government regulation, improve the efficiency of the government, and force the platforms to carefully review the various information data flowing in the platforms to avoid penalties for distorted information. Thus, it is a collaborative gaming process between the two sides.

Unlike traditional game theory, evolutionary game theory assumes humans are finitely rational and usually reach game equilibrium through trial and error. Due to the asymmetry or incompleteness of information, the subject will waver in different strategies to obtain the maximum benefit, and the surrounding subjects or game parties very easily influence its strategy choice. Thus, there is a dynamic adjustment and imitation of the process of others. Interests drive these three parties and eventually make a scientific evolutionary game strategy fit for purpose and operable [40]. Combined with practical research, the evolution process of DSG requires the participation of the central government, local governments, and platforms, the impossibility of complete rationality of each subject of interest, and the mutual influence of their strategic choices, which is a dynamic evolution of the behavior of all parties adjusting each other under certain rules [41]. Therefore, this paper adopts evolutionary game theory and numerical simulation to analyze the dynamic game process of DSG. Constructing a three-party evolutionary game model of the central government, local governments, and platforms determines the evolutionary and stabilization strategies of the three parties to reach the ideal state in different situations. It provides decision-making references for creating a good digital ecology.

3.2. Model Construction

3.2.1. Participants. This study assumes that the game involves three players, i.e., the central government, the local governments, and the third-party platforms, and that all three parties are finite and rational participants who continuously adjust their strategic choices over time to maximize their benefits.

3.2.2. Behavioral Strategies. From the platforms' perspective, there are two primary strategies for implementing cybersecurity measures: "active governance" and "negative governance." Active governance means they may implement cyberspace security strategies, strengthen the process of collecting, transmitting, storing, using, sharing, and destroying relevant data in the platforms' daily operation, actively manage hidden dangers in data, and eliminate environmental externalities generated by themselves. On the other hand, negative governance means they may neglect the effective protection and reasonable use of the organization's data to save governance costs.

From the local governments' perspective, adopting a "participation" strategy involves monitoring and auditing the implementation of data security regulations, policies, and norms on platforms, intervening when necessary to address issues like data theft and illegal transactions. This approach aims to reduce the frequency of data security incidents and minimize the impact of negative public opinion, thereby enhancing government credibility. However, if regulatory intervention is not timely due to technological immaturity or high costs, a "non-participation" strategy may be chosen.

From the central government's perspective, the "emergency response" strategy serves as the last line of defense for digital security governance. This involves implementing emergency measures to counter data security threats and attacks promptly. While this strategy aims to minimize the negative impact of data security incidents, it may face limitations due to the complexity and ambiguity of data issues. In such cases, a "non-emergency response" strategy might be adopted after weighing factors like government image, economic interests, and social stability, opting for a more moderate approach instead of immediate emergency action.

The relationship among the digital ecosystem and platforms adopting proactive governance strategies, local governments implementing participatory management strategies, and the central government employing emergency response strategies for data crises is one of interdependence and collaboration. Each entity plays a distinct yet complementary role in fostering an open, healthy, and secure digital environment.

Platforms' Governance Strategies. Platforms' proactive governance strategies contribute to maintaining a healthy digital ecosystem by implementing measures such as self-regulation, enhancing data protection, and optimizing algorithms and content moderation. These efforts aim to prevent issues before they escalate, reducing the need for intervention by local or central governments.

Local Governments' Participatory Management Strategies. Local governments engage in participatory management to provide tailored, region-specific governance within the digital ecosystem. Strategies may include promoting digital literacy, strengthening local regulatory capacities, and assisting platforms in enforcing national policies. This collaborative approach complements efforts by central authorities and platforms.

Central Government's Emergency Response to Data Crises. In the event of data breaches, cyberattacks, or other emergencies, the central government's role becomes pivotal. With greater resources and authority, the central government can swiftly address cross-platform and cross-regional issues, safeguarding public interests and national security.

The stability of this framework depends on effective implementation, communication, and coordination among the involved parties. While inherently stable in theory, its practical stability hinges on factors such as adaptability to evolving challenges and the establishment of robust communication channels and coordination mechanisms. Continuous monitoring, evaluation, and strategy refinement are essential for maintaining stability within the digital ecosystem. The DSG tripartite game strategy constructed in this paper is shown in Figure 1.

3.2.3. Model Hypothesis

H1. All interested parties are finitely rational. Third-party platforms have two strategies: "active governance" and "negative governance," with the probabilities being x and $1-x$, respectively. The local governments and the central government also have two strategies: the former is "participation" and "non-participation," with a probability of y and $1-y$, while the latter is "emergency response" and "non-emergency response," with probabilities of z and $1-z$, where $0 \leq x, y, z \leq 1$.

H2. The probability of a data security incident is p, which will lead to platforms' loss q (including direct income loss and compensation payable) and local governments' fine f. At the same time, the central government will also collect a fine e from local governments due to poor management.

H3. When platforms neglect the importance of data security by adopting a passive governance strategy, it incurs its usual revenue and cost, denoted as $R0$ and $C0$, respectively. However, if the platforms actively engage in digital security governance, it incurs additional costs in technology, management, operations, and maintenance, denoted as $C1$. Alongside this, there are implicit benefits such as enhanced security, reputation, and access to political resources, denoted as R, resulting in positive externalities that boost the credibility of local governments (w) and overall societal benefits (A). During collaborative efforts between local governments and platforms to review data information, there are costs involved in terms of manpower, resources, and finances ($C2$), partly offset by subsidies provided by the central government (n). In the event of a data security incident with relatively moderate impact and importance, or if the central government deems it unnecessary for urgent intervention after considering factors like governmental image, economic interests, and social stability, it may opt for a "non-emergency response" strategy and handle the situation according to routine plans. However, if the central government chooses not to respond urgently from a broader perspective, it may lead to misunderstandings and dissent among other stakeholders, resulting in disharmony, destabilization of society, and reputational damage, denoted as environmental negative externalities (T). On the other hand, if there is damage to critical data compromising public or national interests, the central government would need to implement an emergency response strategy. In addition to the usual "non-emergency response," this might require additional funding for specialized data recovery and repair work, including costs for data recovery software, services, hiring external consultants, and experts for technical support and consultancy, denoted as $C3$. However, this would also help mitigate losses for the platforms and local and central governments, denoted as $u1$, $u2$, and $u3$, respectively.

Table 1 reports the parameters of the above assumptions, and Table 2 presents the game benefit matrix for the DSG process of the platforms, local governments, and central government.

4. Analysis of the Evolutionary Stability Strategy

4.1. Stability Analysis of Subjects

4.1.1. Third-Party Platforms. The expected benefits of the platforms preferring to select "active governance" strategies are $U11$.

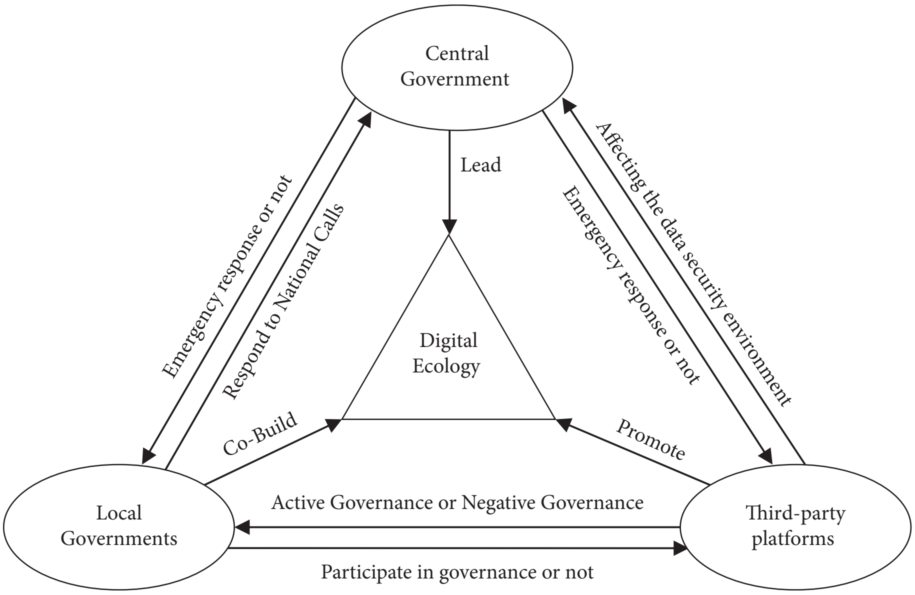

Central Government
Lead
Digital Ecology
Emergency response or not
Respond to National Calls
Affecting the data security environment
Emergency response or not
Co-Build
Promote
Local Governments
Third-party platforms
Active Governance or Negative Governance
Participate in governance or not

Figure 1: Structure of the tripartite game of DSG.

Table 1: Parameter setting of the tripartite game model.

Stakeholders	Symbols	Descriptions
Platforms	$R0$	Baseline returns in the case of negative governance
	$C0$	Baseline costs in negative governance
	$C1$	The technical, management, operational, and maintenance costs invested in active governance
	R	The hidden benefits, such as corporate reputation and business security generated by active governance
	q	Direct or indirect losses to the platforms caused by data security issues
	f	Fines paid by platforms to local governments after data security issues
	p	Probability of data security issues
Local governments	$C2$	The human, financial, and material costs of participating in DSG
	n	Subsidies provided by the central government for local governments to participate in governance in response to national policies
	e	Local fines paid to the central government after a data security issue
	w	The benefit to local credibility of platforms actively maintaining data security
Central government	$C3$	The additional technical and human cost of adopting the "emergency response" strategy over the "non-emergency response"
	$u1$	The loss recovered for platforms in emergency response to data security crisis
	$u2$	The loss recovered for the locality in emergency response to data security crisis
	$u3$	The loss recovered for the community at large in the emergency response to the data security crisis
	T	Negative environmental externality losses caused by "non-emergency response"
	A	The overall benefit of active governance of the platforms to society

$$\begin{aligned} U11 &= yz(R0 + R - C0 - C1 - p(q + f - u1)) + y(1 - z)(R0 + R - C0 - C1 - p(q + f)) \\ &\quad + z(1 - y)(R0 + R - C0 - C1 - p(q - u1)) + (1 - y)(1 - z)(R0 + R - C0 - C1 - pq) \\ &= R - C1 - C0 + R0 - pq - fpy + zpu1. \end{aligned} \tag{1}$$

The expected benefits of the platforms select "negative governance" strategies are $U12$.

Table 2: Benefit matrix for the three-party game.

	Platforms	Local governments	Central government
(x, y, z)	$R0 + R - C0 - C1 - p(q + f - u1)$	$p(f + u2) - C2 + n + w$	$A - n + pu3 - C3$
$(x, y, 1 - z)$	$R0 + R - C0 - C1 - p(q + f)$	$pf - C2 + n + w$	$A - n - pT$
$(x, 1 - y, z)$	$R0 + R - C0 - C1 - p(q - u1)$	$p(-e + u2) + w$	$A + p(e + u3)$
$(x, 1 - y, 1 - z)$	$R0 + R - C0 - C1 - pq$	w	$A - pT$
$(1 - x, y, z)$	$R0 - C0 - p(q + f - u1)$	$p(f + u2) + n - C2$	$-n + pu3 - C3$
$(1 - x, y, 1 - z)$	$R0 - C0 - p(q + f)$	$pf + n - C2$	$-n - pT$
$(1 - x, 1 - y, z)$	$R0 - C0 - p(q - u1)$	$p(-e + u2)$	$p(e + u3)$
$(1 - x, 1 - y, 1 - z)$	$R0 - C0 - pq$	0	$-pT$

$$\begin{aligned}U12 &= yz(R0 - C0 - p(q + f - u1)) + y(1 - z)(R0 - C0 - p(q + f)) + (1 - y)z(R0 - C0 - p(q - u1))\\ &\quad + (1 - y)(1 - z)(R0 - C0 - pq) = R0 - C0 - pq - fpy + zpu1.\end{aligned} \tag{2}$$

The average expected benefits of the platforms are $U1$.

$$U1 = xU11 + (1 - x)U12 = R0 - C0 - C1x + Rx - pq - fpy + zpu1. \tag{3}$$

Therefore, according to Taylor's model [42], the replicator dynamic equation is as follows:

$$\begin{aligned}F(x) &= \frac{dx}{dt} = x(U11 - U1) = x(1 - x)(U11 - U12)\\ &= x(C1 - R)(x - 1).\end{aligned} \tag{4}$$

Based on the stability theorem of the differential equation, the conditions that make the probability of the platforms choosing active governance in a steady state are $F(x) = 0$ and $(dF(x)/dx) < 0$. Therefore, solving for the first-order derivative of $F(x)$ reveals that when $C1 < R$, $(dF(x)/dx) = 1 - 2x$, $(dF(x)/dx)|_{x=0} > 0$, and $(dF(x)/dx)|_{x=1} < 0$, so $x = 0$ is the stable point. When $C1 > R$, $(dF(x)/dx) = 2x - 1$, $(dF(x)/dx)|_{x=0} < 0$, and $(dF(x)/dx)|_{x=1} > 0$, so $x = 1$ is the only ESS.

4.1.2. Local Governments. The expected earnings when local governments choose "participation" strategies are $U21$.

$$\begin{aligned}U21 &= xz(p(f + u2) - C2 + n + w) + x(1 - z)(pf - C2 + n + w) + (p(f + u2) + n - C2)(1 - x)z\\ &\quad + (1 - x)(1 - z)(pf + n - C2) = n - C2 + fp + wx + pu2z.\end{aligned} \tag{5}$$

The expected earnings when local governments choose "non-participation" strategies are $U22$.

$$\begin{aligned}U22 &= xz(p(-e + u2) + w) + x(1 - z)w + (1 - x)z(p(-e + u2))\\ &= wx - epz + pu2z.\end{aligned} \tag{6}$$

The average earnings for local governments are $U2$.

$$\begin{aligned}U2 &= yU21 + (1 - y)U22\\ &= ny - C2y + wx - epz + fpy + pu2z + epyz.\end{aligned} \tag{7}$$

The replicator dynamic equation is as follows:

$$F(y) = \frac{dy}{dt} = y(U21 - U2) = y(1 - y)(U21 - U22) = y(1 - y)(n - C2 + fp + epz). \tag{8}$$

If $z = ((C2 - n\text{—fp})/\text{ep})$, then for any y, $F(y) \equiv 0$, and thus axis y is in a stable state, and any governance strategy of local governments is a stable strategy. If $z \neq ((C2 - n \text{— fp})/\text{ep})$, then we solve for $F(y) = 0$ and the derivative of $F(y)$, for two solutions $y = 0$ and $y = 1$ of equation (8), $(dF(y)/dy) = (1 - 2y)(n - C2 + fp + epz)$.When $z < ((C2 - n\text{—fp})/\text{ep})$, $(dF(y)/dy)|_{y=0} < 0$, $(dF(y)/dy)|_{y=1} > 0$, $y = 0$ is the only ESS, and the stability strategy of the local governments is not to participate in the DSG process of the third-party platforms. When $z > ((C2 - n\text{—fp})/\text{ep})$, $(dF(y)/dy)|_{y=0} > 0$, $(dF(y)/dy)|_{y=1} < 0$, $y = 1$ is the only ESS, and the local governments choose to participate in the DSG process.

4.1.3. Central Government. Let $U31$ and $U32$, respectively, denote the expected benefits of the central government's choice of "emergency" and "non-emergency" strategies.

$$\begin{aligned} U31 &= xy(A - n + pu3 - C3) + x(1 - y)(A + p(e + u3)) + (1 - x)y(-n + pu3 - C3) + (1 - x)(1 - y)(+p(e + u3)) \\ &= Ax - C3y + ep + pu3 - ny - epy, \end{aligned} \tag{9}$$

$$\begin{aligned} U32 &= xy(A - n - pT) + x(1 - y)(A - pT) + (1 - x)y(-n - pT) \\ &\quad + (1 - x)(1 - y)(-pT) = Ax - Tp - ny. \end{aligned} \tag{10}$$

The average expected benefits of the platforms are $U3$.

$$\begin{aligned} U3 = zU31 + (1 - z)U32 &= (z - 1)(x(A - Tp)(y - 1) - y(x - 1)(n + Tp) + xy(n - A + Tp) + (x - 1)(y - 1)Tp) \\ &\quad + z(y(x - 1)(C3 + n - pu3) - x(A + p(e + u3))(y - 1) + xy(A - C3 - n + pu3) + p(e + u3)(x - 1)(y - 1)). \end{aligned} \tag{11}$$

The replicator dynamic equation is as follows:

$$\begin{aligned} F(z) &= \frac{dz}{dt} = z(U31 - U3) \\ &= z(1 - z)(Tp - C3y + ep + pu3 - epy). \end{aligned} \tag{12}$$

If $y = (Tp + ep + pu3)/(C3 + ep)$, then for an arbitrary z, $F(z) \equiv 0$, and then axis z is in a stable state, and any response strategy of the central government is a stable strategy. If $y \neq (Tp + ep + pu3)/(C3 + ep)$, then we solve for $F(z) = 0$ and the derivative of $F(z)$, for two solutions $z = 0$ and $z = 1$ of equation (12), $(dF(z)/dz) = (1 - 2z)(Tp - C3y + ep + pu3 - epy)$. When $y < (Tp + ep + pu3)/(C3 + ep)$, $(dF(z)/dz)|_{z=1} < 0$, $(dF(z)/dz)|_{z=0} > 0$, $z = 1$ is the only ESS, and the stability strategy of the central government is to respond to possible data security issues promptly. When $y > (Tp + ep + pu3)/(C3 + ep)$, $(dF(z)/dz)|_{z=1} > 0$, $(dF(z)/dz)|_{z=0} < 0$, $z = 0$ is the only ESS, and the central government does not respond in time.

4.2. Stability Analysis of the System. The research object of the replication dynamic equations in an evolutionary game is a certain group, and thus, a single group's evolutionary stability strategy (ESS) cannot represent the whole system. Hence, the Jacobian matrix is constructed. Specifically, we find the partial derivatives of $F(x)$, $F(y)$, and $F(z)$ about x, y, and z, respectively, and then the construct the Jacobian matrix of the tripartite game, as presented below:

$$\begin{aligned} J = \begin{bmatrix} j_{11} & j_{12} & j_{13} \\ j_{21} & j_{22} & j_{23} \\ j_{31} & j_{32} & j_{33} \end{bmatrix} &= \begin{bmatrix} \dfrac{\partial F(x)}{\partial x} & \dfrac{\partial F(x)}{\partial y} & \dfrac{\partial F(x)}{\partial z} \\[2ex] \dfrac{\partial F(y)}{\partial y} & \dfrac{\partial F(y)}{\partial y} & \dfrac{\partial F(y)}{\partial z} \\[2ex] \dfrac{\partial F(z)}{\partial x} & \dfrac{\partial F(z)}{\partial y} & \dfrac{\partial F(z)}{\partial z} \end{bmatrix} \\ &= \begin{bmatrix} (C1 - R)(2x - 1) & 0 & 0 \\ 0 & (1 - 2y)(n - C2 + fp + epz) & epy(1 - y) \\ 0 & z(z - 1)(C3 + ep) & (1 - 2z)(Tp - C3y + ep + pu3 - epy) \end{bmatrix}. \end{aligned} \tag{13}$$

Let $F(x) = 0$, $F(y) = 0$, and $F(z) = 0$, which can provide eight pure strategy equilibria as well as two mixed strategy equilibria: $\mathrm{E}(1,1,1)$, $\mathrm{E}(1,1,0)$, $\mathrm{E}(1,0,1)$, $\mathrm{E}(1,0,0)$, $\mathrm{E}(0,1,1)$, $\mathrm{E}(0,1,0)$, $\mathrm{E}(0,0,1)$, $\mathrm{E}(0,0,0)$, $\mathrm{E}(0, (Tp + ep + pu3)/(\mathrm{C3 + ep}), (\mathrm{C2 - n - fp/ep}))$, and $\mathrm{E}(1, (Tp + ep + pu3)/(\mathrm{C3 + ep}), (\mathrm{C2 - n - fp/ep}))$. According to the Lyapunov stability condition, the equilibrium point is asymptotically stable when the real parts of the eigenvalues of the Jacobi matrix are less than zero [37]. Calculating the Jacobi matrix's eigenvalues for each equilibrium point separately provides the condition that each equilibrium point is an evolutionary game ESS, as reported in Table 3.

Because $Tp + C3 + pu3 > 0$ and $i > 0$, $\mathrm{E}(1,0,0)$, $\mathrm{E}(0,0,0)$, $\mathrm{E}(0, (Tp + ep + pu3)/(\mathrm{C3 + ep}), ((\mathrm{C2 - n - fp})/\mathrm{ep}))$, and $\mathrm{E}(1, (\mathrm{Tp + ep + pu3})/(\mathrm{C3 + ep}), ((\mathrm{C2 - n - fp})/\mathrm{ep}))$ do not satisfy the conditions of ESS. To sum up, in the tripartite evolutionary game model, only $\mathrm{E}(0,1,1)$, $\mathrm{E}(0,1,0)$, $\mathrm{E}(0,0,1)$, $\mathrm{E}(1,1,0)$, $\mathrm{E}(1,0,1)$, and $\mathrm{E}(1,1,1)$ can be transformed into a stabilization strategy under certain conditions, while the decision-making behavior of third-party platforms, local governments, and central government is determined by $R - C1, n + fp - C2$, and $Tp - C3 + pu3$. Besides, $R - C1$ denotes the excess profit between the hidden benefits derived from active governance by the third-party platforms and the costs paid, $n + fp - C2$ is the excess profit between the subsidies received by the local governments for participating in governance, the fines collected, and the cost of its inputs, and $Tp - C3 + pu3$ represents the difference between the losses recovered and the costs incurred by the central government in responding to the data crisis in time. Table 3 highlights that the values of $C2 - n - fp$ may fall within the three intervals: $-\infty, 0$, $0, ep$, and $ep, +\infty$, while the interval ranges of $R - C1$ and $Tp - C3 + pu3$ are both $-\infty, 00, +\infty$.

(1) When $R - C1 \in -\infty, 0$, for third-party platforms, the additional benefits of choosing active governance are less than the technical, management, operational, and other costs invested in this area in the early stage. At this point, negative governance will become the platforms' priority choice. When $R - C1 \in 0, +\infty$, the hidden benefits of active governance are higher than the costs involved, and the platforms are more inclined to active governance.

Therefore, safeguarding the governance benefits of third-party platforms can effectively prevent platforms from treating data security issues negatively and instead take preventive measures to strengthen the management and governance of data security, making the stable decision-making level of platforms from $x = 0$ to $x = 1$. The government can increase the net income of platforms governance by giving subsidies or awarding them through official websites or media reports to expand the reputation of the platforms, increase their willingness to actively govern, effectively prevent improper data processing practices, better protect the security of national digital assets, further improve the quality and efficiency of digital services, and promote the construction of digital ecological security.

(2) When $C2 - n - fp \in -\infty, 0$, the subsidies received and the fines collected by local governments for participating in the DSG process are higher than the costs they pay. Thus, participation in governance is the best strategy for local governments. When $C2 - n - fp \in -\infty, 0 \cup 0, ep$, the expected penalty imposed on the local governments by the central government in response to a data breach is higher than the cost paid by the local governments for participating in governance. Thus, participation in governance will be the optimal choice to avoid punishment at a higher level. When $C2 - n - fp \in ep, +\infty$, the participation cost is higher than the potential penalties, and the local governments' stabilization strategy becomes "non-participation," which is not conducive to the stable development of the digital ecology.

When the benefits of the local governments' refusal to participate in governance are greater, the central government should strengthen the penalties for the local government's negligence. Higher administrative penalties can encourage them to strictly fulfill their data governance responsibilities and improve local governments' governance. In addition, through the appropriate use of financial subsidy policies, it can alleviate local conflicts caused by interest relations, improve the motivation of local governments, increase their intention to participate, and make local governments' stable decisions from $y = 0$ to $y = 1$ evolution, thus effectively ensuring the availability and security of local data resources, thereby maintaining the stable operation of the digital ecology and public security.

(3) When $Tp - \mathrm{C3 + pu3} \in -\infty, 0$, if the cost for the central government to take emergency measures against an occurring data security problem is much higher than its negative externality loss, then the central government will tend to adopt a non-emergency strategy. When $Tp - C3 + pu3 \in 0, +\infty$, the severity of the set of consequences caused by a data security problem far outweighs the cost to the central government of activating an emergency response. The central government will pay more attention to the emergency response process of a data security incident to achieve prevention and control of cyberattacks, disinformation, and other digital risks and reduce the damage caused to the digital ecology.

To sum up, there are six possible stability points in the DSG game system, of which $\mathrm{E}(1,1,1)$ is the ideal stability point, corresponding to the ideal strategy combination of "active governance, participation, and emergency response." Different conditions correspond to different combinations

Table 3: Equilibrium point and eigenvalue of the system.

Equilibrium point	λ_1	λ_2	λ_3	State
$E(0,0,0)$	α	$-\beta$	$\gamma + C3 + ep$	Unstable $(\lambda_3 > 0)$
$E(0,1,0)$	α	β	γ	$\alpha, \beta, \gamma < 0$
$E(0,0,1)$	α	$ep - \beta$	$-\gamma - C3 - ep$	$\alpha < 0,\ ep - \beta < 0$
$E(0,1,1)$	α	$\beta - ep$	$-\gamma$	$\alpha, -\gamma, \beta - ep < 0$
$E(0, Tp + ep + pu3/C3 + ep, (C2 - n - fp/ep))$	α	i	$-i$	Unstable $(\lambda_2 > 0)$
$E(1,0,0)$	$-\alpha$	$-\beta$	$\gamma + C3 + ep$	Unstable $(\lambda_3 > 0)$
$E(1,1,0)$	$-\alpha$	β	γ	$-\alpha, \beta, \gamma < 0$
$E(1,0,1)$	$-\alpha$	$ep - \beta$	$-\gamma - C3 - ep$	$-\alpha, ep - \beta < 0$
$E(1,1,1)$	$-\alpha$	$\beta - ep$	$-\gamma$	$\beta - ep, -\alpha, -\gamma < 0$
$E(1, (Tp + ep + pu3)/(C3 + ep), (C2 - n - fp/ep))$	$-\alpha$	i	$-i$	Unstable $(\lambda_2 > 0)$

$\alpha = R - C1, \beta = C2 - n - fp, \gamma = Tp - C3 + pu3,$ and $i = (-e(C3 + ep)(Tp - C3 + pu3)(T + e + u3)(n - C2 + fp)(n - C2 + ep + fp))^\wedge(1/2)/(pe^\wedge 2 + C3e)$.

of strategies. Obviously, in order for E(1, 1, 1) to be ESS, it must satisfy three conditions simultaneously: $C1 - R < 0$, $C2 - n - fp - ep < 0$, and $C3 - pu3 - Tp < 0$, i.e., the cost of maintaining data security for the platforms is less than the hidden benefits they receive, the cost of participating in governance for the local governments is less than the subsidies and fines, and the cost of emergency responding to a data security incident for the central government is less than the negative externalities caused by the continued fermentation of the incident.

5. Numerical Simulation and Discussion

In order to discuss the sensitivity of the parameters and verify the model's accuracy, we used MATLAB 2022b to simulate the dynamic evolutionary trajectory of the evolving system. Considering the research hypothesis of this paper, by drawing on [40, 43–45] and based on the evolutionary stability strategies (active governance, participation, and emergency response), the parameters of the diverse cases are set as follows: $R = 9, C1 = 8, p = 0.4, C2 = 5, n = 4, f = 2$, $T = 20, C3 = 8, u3 = 4, e = 6$. In the previous discussion, we have analyzed how the decision making of third-party platforms, local governments, and the central government is determined by factors such as $R - C1, n + fp - C2,$ and $Tp - C3 + pu3$. It is evident that R and $C1$, as well as n and f, represent conflicting interests. For instance, an increase in R implies a decrease in $C1$, both indicating an increase in benefits. These factors are essentially of the same nature, with their evolutionary states in the simulation graph being inversely related. Therefore, focusing on factors of different nature, let us now primarily examine how R, n, p, T, and $C3$ influence the evolutionary trajectory of the digital security governance system. When analyzing the sensitivity of a certain parameter, the values of other parameters remain the same.

5.1. Implicit Benefits. Let R be 1, 9, and 15, respectively, and we observe the simulation results of its evolution from the initial time 0 to 50. According to Figure 2, when $R < 9$, x converges from 0.2 to 0, and the DSG system degrades to E(0, 1, 1), which means a poor state. As R increases, the willingness x of the platforms to govern grows gradually. In other words, x converges from 0.2 to 1 after a long period of evolution. Finally, the system evolves to E(1, 1, 1). This is because when the platforms are actively governed, they effectively safeguard the security of commercial secrets, personal privacy, and other information, reducing legal risks and increasing user trust and stickiness, improving the platforms' reputation, influence, and market competitiveness. Therefore, the benefits of governance positively affect the behavioral choices of the platforms, and the more cost-effective the platforms' governance investment is, the greater the probability of active governance is.

5.2. Government Subsidies. Figure 3 highlights that the probability of the local governments choosing the participation strategy converges to 0 when $n < 5$ and converges to 1 when $n > 5$. The simulation results indicate that increasing the number of local government subsidies significantly improves their willingness to participate in governance and positively affects the development of data ecology. Therefore, as rational economic agents, local governments may take advantage of the governance benefits if the governance costs are too high and share the economic benefits of governance brought by other parties without actively taking precautionary measures. Meanwhile, the system degenerates to the unstable state of E(1, 0, 1). When the central government, whose subsidies are in the medium to high range, supports local governments in maintaining data information security, local governments will actively participate in the DSG process.

5.3. Contingency Costs and Negative Externality Losses. Let C3 be 3, 8, and 20 while T be 5, 20, and 35. These values represent the observed effects of three different strategies on three participants, as illustrated in Figures 4(a) and 4(b). Figure 4 reveals that when $\mathrm{C3} \leq 8$ or $T > 20$, y rapidly converges from 0.2 to 1 after evolution, and the convergence rate increases significantly. Undoubtedly, the central government tends to adopt the emergency response strategy, which means the system has evolved to an ideal stable state E(1, 1, 1) that continuously promotes the healthy development of digital ecology. When $C3$ increases or T decreases, the probability of adopting an emergency response strategy decreases, but z does not reduce below its initial willingness

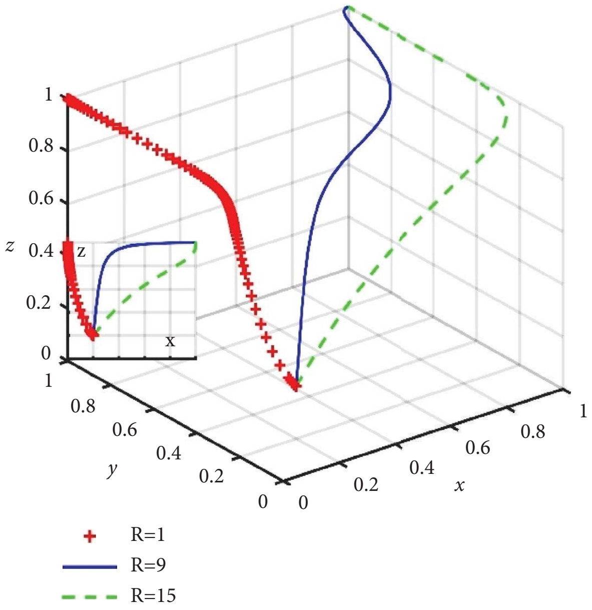


Figure 2: Sensitivity of hidden benefits.

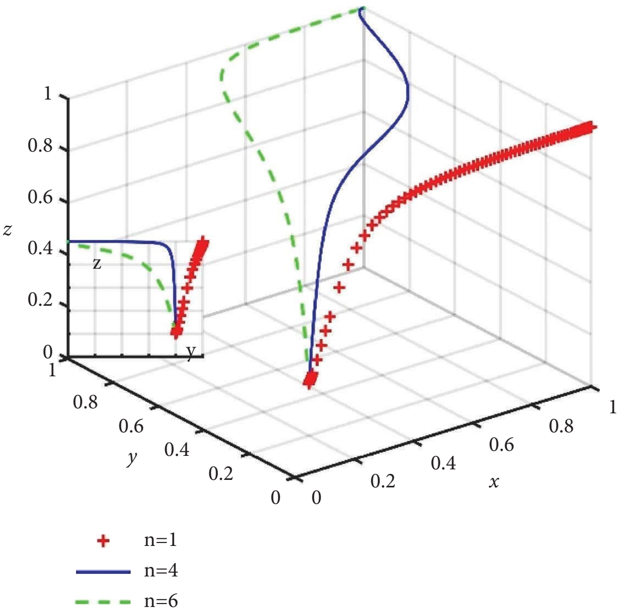
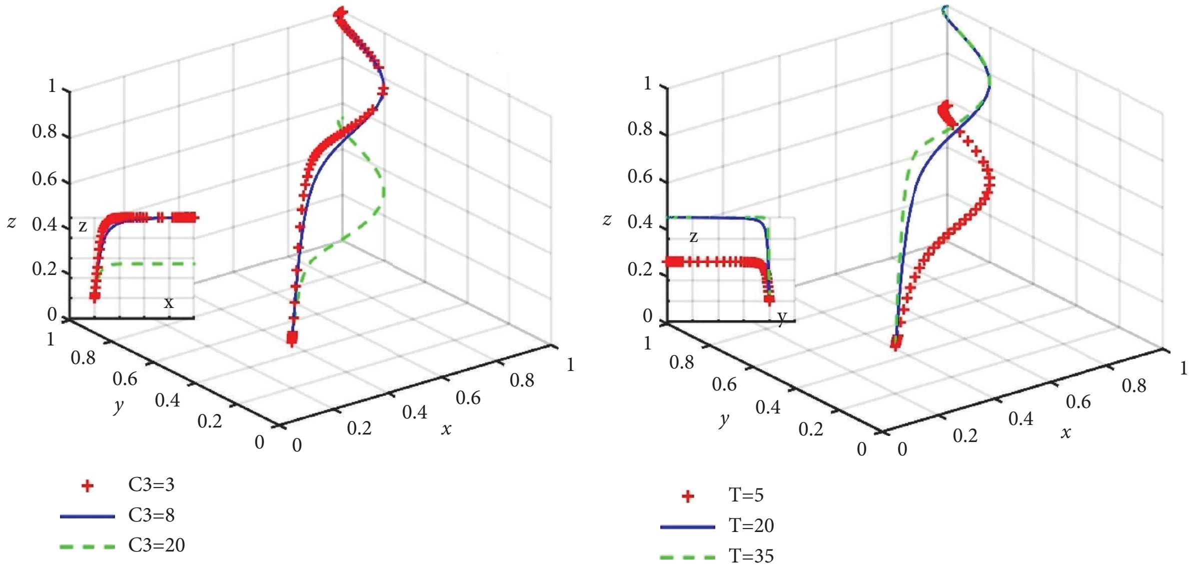


Figure 3: Sensitivity of government subsidies.

probability. Unless the cost of response is much higher than the negative externality loss and the amount tends to infinity, the system will degrade to the poor stability $E(1,1,0)$. The central government has sufficient financial capacity to bear the lower costs. Moreover, based on the overall welfare of society, the central government will not let data problems exist due to the loss of its interests. Even if coping costs are increasing, it will respond in time. However, when the emergency cost increases excessively, far below the negative externalities caused by the risk of data leakage, which seriously affects the allocation of national financial resources, the central government will tend to be an emergency response.

5.4. Probability of Data Security Events. Let p be 0.1, 0.2, 0.4, and 0.6, and we observe its influence on the strategy choice of the three subjects, and the relevant situation can be



(a)

(b)

Figure 4: Sensitivity analysis of contingency costs and negative externality losses. (a) Sensitivity of contingency costs and (b) sensitivity of negative externality losses.

obtained in Figure 5, in which the horizontal axis indicates the growth of time, and the vertical axis indicates the probability that the platforms, local governments, and the central government choose to adopt the corresponding strategy. Figure 5 reveals that p has significantly different degrees of impact on platforms, local governments, and central government. Overall, when $p = 0.1$ or 0.2 (low range), the probability of data security incidents positively affects the platforms and central government behavior and negatively affects the governance behavior of local governments, whose states are unstable. When $p = 0.4$ or 0.6 (middle to high range), the three entities have reached the positive stable state, suggesting that a higher data crisis will prompt all parties to interrupt threatening events actively. Besides, as p increases, the strategy evolution of the platforms remains unchanged, and z rapidly converges from 0.2 to 1 after evolution, while y first rises and then decreases and then gradually converges from 0 to 1.

This highlights that after the platforms enable satisfactory returns through active governance, regardless of the crisis probability, they will take the initiative to assume the main responsibility of DSG and build a solid foundation for a good data ecological environment. Although the local governments will obtain more self-interest benefits by choosing non-participation, as the probability of data security problems increases, platforms alone may not provide security for data assets in the domain. Therefore, local governments tend to participate in governance. Given that the time to reach the steady state will gradually shorten, at low crisis probabilities, the central government can involve local governments in the governance process through standard controls, official media coverage, punitive interventions [46], or coercive measures to reduce the phenomenon of "free-riding."

5.5. Chapter Summary. Through an extensive review of literature, research reports, and numerical simulation, this study has summarized the theoretical outcomes of digital security governance. Previous studies on data security mainly focused on stakeholders such as government regulators and data attackers like hackers or internal employees. In contrast, this study primarily analyzes the governance entities. Key factors that influence behavior strategies were also considered, including the cost of investment and the severity of penalties, which are common to previous research. However, due to the different stakeholders considered, the key factors influencing behavior strategies also differ. The innovations in this study are as follows:

(1) *Innovative Research Focus.* Traditional studies often viewed the government as a single entity, while this study introduces the concepts of central and local governments. It builds a novel tripartite evolutionary game model consisting of "third-party platforms, local governments, and the central government," aiming to better consider the unique responsibilities and roles of different levels of government in digital security governance. By defining the roles and responsibilities of local and central governments in digital security governance, stakeholders can minimize confusion, duplication of effort, and jurisdictional conflicts. This approach aids in effective decision making, streamlining operational processes, and enhancing the overall efficiency and

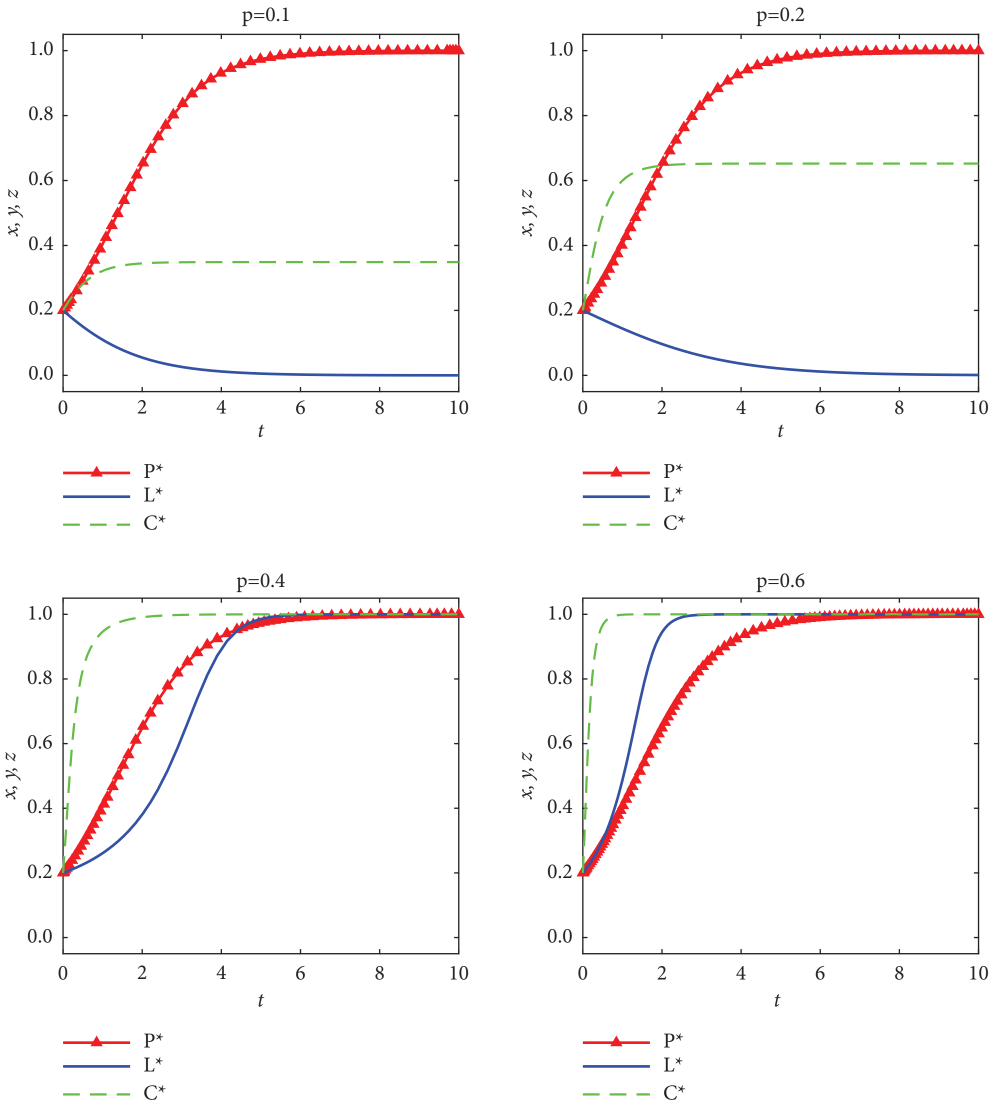


Figure 5: Sensitivity of data security event probability.

effectiveness of governance mechanisms. Moreover, this study not only explores the interaction between the government and other stakeholders but also considers the game relationship within the government. By incorporating internal dynamics of the government, this analysis method increases the complexity of the game, enabling a more nuanced analysis of factors that influence internal decision-making processes and policy formulation. By considering the roles and interactions among these government entities, this study provides a new perspective on the dynamics of digital security governance.

(2) *Innovative Factors of Influence*. This study specifically focuses on key factors influencing the behavior strategies of the central government, aiming to accurately assess its decision-making process and understand its actions in the context of digital security governance. Firstly, it considers the environmental negative externalities associated with adopting "non-emergency responses." In the process of digital security governance, the central government may need to weigh the potential negative impacts of security incidents or threats against the benefits of implementing emergency response measures. Secondly, it considers the additional technological and manpower costs associated with adopting "emergency response" strategies. After a sudden data security incident, the central government may need to allocate significant resources for developing technical tools, training personnel, and engaging in activities related to incident response. Lastly, this study also focuses on the losses that can be recovered by adopting "emergency response" strategies. When the central government takes swift action to respond to data security incidents, it may mitigate or even prevent economic, reputational, and trust losses for stakeholders. This

study innovatively analyzes the impacts of these sensitive factors on the central government's decision-making process from the perspectives of environmental negative externalities, emergency response costs, and recoverable losses. These research innovations aim to provide government decision makers with comprehensive and accurate information to formulate targeted and feasible digital security governance strategies, promoting sustainable development in data security.

6. Conclusions and Implications

6.1. Conclusions. Data security is the foundation of the digital ecology, without which the digital ecology will not function properly. Indeed, DSG can effectively protect the country's digital assets, prevent risks such as data leakage, tampering, and damage, improve the ability of each subject to respond to information security risks, and reduce the occurrence of security incidents to guarantee the stable development of each subject. This paper carefully examines the heterogeneous impact of different factors on DSG in China based on the current context of creating a digital ecology. Furthermore, this study helps to promote the benign construction of digital ecology and reform the DSG mechanism in China. In addition, it has important practical significance and application value for protecting the interests of individuals and organizations, preventing data leakage and abuse, and maintaining social order and stability.

Research indicates that key parameters such as implicit benefits, government subsidies, and negative externalities play a significantly positive role in the development of digital ecosystems within the framework of digital security governance. These parameters, within certain ranges, can positively support the ideal behavior strategies of various stakeholders, evolving to a stable state:

(i) Increasing implicit benefits can promote third-party platforms to actively govern data security. Therefore, enhancing the benefits of platforms digital security governance and reducing governance costs is an effective way to prevent platforms from relaxing governance efforts.

(ii) Financial subsidies from the central government to local governments can effectively enhance the latter's participation in governance, which is crucial for its stability. However, for subsidies to be effective, the subsidy amount must exceed the sum of the costs incurred by local governments in governing data security and the fines they receive, ensuring the safeguarding of data security in an evolving and stable market environment.

(iii) Low negative externalities and high emergency costs reduce the probability of the central government opting for an emergency response to data security threats. However, as the central government is responsible for protecting public interests and national security, as long as emergency costs are within its capacity, the central government will tend to adopt an "emergency response" strategy.

Additionally, the probability of data security incidents also affects digital ecosystems, leading to two main scenarios:

(i) When the probability is low, indicating a stable market environment with a low likelihood of data security incidents, platform strategies lean towards active governance, while local governments adopt a passive governance approach, and the central government's strategy remains undecided.

(ii) When the probability is moderate to high, indicating a volatile market environment with a higher likelihood of data security incidents, all three parties adopt positive behavioral strategies, namely, active governance, participation in management, and emergency response.

Based on the two scenarios described, two different approaches to governance can be discerned. Specifically, (1) Local governments should be regulated more in a stable market environment with a low risk of data crises. The central government's response costs to different data crisis events are different. The higher the emergency response cost, the lower the chance of adopting an emergency response strategy, but the central government is always willing to bear the cost within a certain range due to the consideration of the overall welfare of the society. A secure data environment creates a positive externality whereby local governments will use the resources of others or other organizations for free to achieve their benefits, i.e., the phenomenon of "free-riding." The central government can involve local governments in governance through standard control, official media reports, and punitive interventions or coercive measures. (2) The willingness of platforms and local governments to govern should be increased in a data crisis. The implicit benefits of platforms should be increased, and the amount of subsidies established should exceed the cost of governance for local governments. The platforms' governance strategy choice is positively related to the hidden benefits of security, word-of-mouth reputation, and political resources brought by governance, and its role is significantly more dynamic. In a changing data environment, the higher the invisible gains, the stronger the willingness to govern. Moreover, it is significant for the central government to adopt certain subsidy incentives to increase local willingness to participate in governance and maintain data security. The central government's reward and punishment policies will affect local governments' strategic choices. If the policy subsidies can balance the benefits and costs of governance, the chance of local government's participation in governance is greater, and the more favorable it is to the healthy development of the digital ecology.

There are areas for improvement in this study. Firstly, the game mechanism is relatively simple, without including netizens and other participating subjects; the strategy space is also simplified to a certain extent, and the local government's regulatory obligation is set as the degree of participation in governance without more detailed and in-depth construction, and the complex interaction mechanism behind it is not studied in depth. Moreover, the game participants' behavior analysis validity may be biased since the simulation values are conducted under simulation conditions.

6.2. Implications

6.2.1. Managerial Implication. This paper innovatively substitutes the negative externality loss and the probability of data security events into the cost-benefit matrix and introduces the central government as an important role in improving the governance organizational structure. The evolutionary game of DSG under digital ecological objectives is explored in depth, and by analyzing the interactions and influences between third-party platforms, local governments, and only the central government, it can reveal the key issues and challenges of DSG in the digital era and provide corresponding solutions. Specifically, this study promotes in-depth thinking on important topics such as information sharing, privacy protection, and cybersecurity among different subjects in the digital ecosystem. In addition, exploring the evolutionary game model can help understand and predict the evolutionary trend of DSG mechanisms and provide decision makers with a scientific basis for formulating relevant policies and norms. Besides, it can deepen our understanding of DSG under the goal of digital ecology, promote the development of related fields, and provide useful references for social governance and sustainable development in the digital era.

6.2.2. Practical/Social Implications

(1) The role of invisible benefits such as reputation should be emphasized, and a credit assessment system for data security should be established [47]. For instance, Deephouse [48] used theoretical and empirical analyses to show that reputation is a resource that leads to competitive advantage. Trust and reputation systems are important in providing decision support for Internet intermediary services [49], as DSG efforts can be recorded and fed back in real time and deter ethical risks [50].

Credit information can be disclosed to the public by setting tasks and goals related to DSG and evaluating them based on security reports, virus scans, vulnerability discoveries, and other information released by governors. The platforms will be prompted to pay more attention to DSG, thereby promoting the sustained and healthy development of the digital ecology.

(2) Strengthen the research and development of cutting-edge data security technologies to reduce the probability of data security incidents. Digital technology is an indispensable part of DSG, which can improve the efficiency of the supply chain, reduce operating costs, and provide a more optimal decision-making basis for the digital ecological development strategy [51]. It can also design a more intelligent protection system to achieve full-platform data monitoring, such as content validation, tracing, copyright tracking, and desensitization [52]. It helps enterprises better manage data and protect its security, integrity, and privacy. This can narrow the existence time of security vulnerabilities, reduce the system risk level, optimize the efficiency of data governance and management, and improve data security and protection.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

We would like to acknowledge the support and assistance received during the course of this research. We are grateful for the resources provided by the National Social Science Foundation of China that facilitated our work. Additionally, we appreciate the collaboration and contributions of colleagues and partners who helped make this study possible. This research was funded by the National Social Science Foundation of China (21BGJ037).

References

[1] H. Li and C. Peng, "Good digital ecology and the construction of digital rule system," *E-government*, vol. 3, pp. 31–38, 2022.

[2] W. Min, "Application of network and information security risk monitoring and early warning platform in electric power enterprises," in *Proceedings of the China International Conference on Electricity Distribution (CICED)*, pp. 2718–2721, Tianjin, China, September 2018.

[3] M. Yao, "Strategic options for strengthening economic data regulation on platforms," *Qunzhong*, vol. 8, pp. 49-50, 2021.

[4] B. Maynard, T. Tan, A. Ahmad, T. Ruighaver, and T. Ruighaver, "Towards a framework for strategic security context in information security governance," *Pacific Asia Journal of the Association for Information Systems*, vol. 10, pp. 65–88, 2018.

[5] S. Schinagl, S. Khapova, and A. Shahim, *Tensions that Hinder the Implementation of Digital Security Governance*, Cham, Berlin, Germany, 2021.

[6] S. Schinagl, A. Shahim, and S. Khapova, "Paradoxical tensions in the implementation of digital security governance: toward an ambidextrous approach to governing digital security," *Computers and Security*, vol. 122, Article ID 102903, 2022.

[7] "Data security market research report," 2022, https://www.djyanbao.com/report/detail?id=3326959&from=search_list.

[8] T. Que and Z. Wang, "Global digital security governance and action strategies for China's participation in the eraof digital

economy," *Journal of International Security Studies*, vol. 40, pp. 130–154+158, 2022.

[9] T. Dong, "Research on the data governance of intellectual property," *Journal of Management World*, vol. 38, pp. 109–125, 2022.

[10] S. Schinagl and A. Shahim, "What do we know about information security governance?"From the basement to the boardroom": towards digital security governance," *Information and Computer Security*, vol. 28, no. 2, pp. 261–292, 2020.

[11] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: systematic review," *Computers and Security*, vol. 99, Article ID 102030, 2020.

[12] Y. Fan and X. Zhang, "Paradigm shifts, options and approaches to digital security governance," *E-government*, vol. 4, pp. 114–124, 2022.

[13] M. Al-Ruithe, S. Mthunzi, and E. Benkhelifa, "Data governance for security in IoT and cloud converged environments," in *Proceedings of the 13th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA)*, Agadir, Morocco, December 2016.

[14] W. Hou, Z. Gu, and W. Jing, "Data advantages of platform enterprises and consumer privacy protection-From the perspective of tripartite game between government, platform enterprises and consumers under data empowerment," *Economic Review Journal*, vol. 12, pp. 59–69, 2022.

[15] L. Chen and Q. Ma, "Antitrust regulation of data sharing among platform enterprises," *Journal of Intelligence*, vol. 41, pp. 99–107, 2022.

[16] X. Sheng and D. Guo, "Research on digital security governance in open sharing of scientific data," *Library and Information Service*, vol. 64, pp. 25–36, 2020.

[17] M. Nicho, "A process model for implementing information systems security governance," *Information and Computer Security*, vol. 26, no. 1, pp. 10–38, 2018.

[18] T. Ruighaver, "Information security governance: a case study of the strategic context of information security," in *Proceedings of the Pacific Asia Conference on Information Systems*, Langkawi, Malaysia, October 2017.

[19] B. AlKnawy, Z. Kozlakidis, S. Tarkoma et al., "Digital public health leadership in the global fight for health security," *BMJ Global Health*, vol. 8, no. 2, Article ID e011454, 2023.

[20] J. Gabriel, S. M. A. Latheef, and V. Jayavardhanavelu, "Issues on management and governance of data security in HEIs," *Journal of Trend in Scientific Research and Development*, vol. 1, 2018.

[21] L. Masilela and D. Nel, "The role of data and information security governance in protecting public sector data and information assets in national government in South Africa," *Africa's Public Service Delivery and Performance Review*, vol. 9, no. 1, 2021.

[22] S. Karkoskova, "Data governance model to enhance data quality in financial institutions," *Information Systems Management*, vol. 40, no. 1, pp. 90–110, 2023.

[23] Q. Gong, M. Ban, and Y. Zhang, "Blockchain, enterprise digitalization and supply chain finance Innovation," *Journal of Management World*, vol. 37, pp. 22–34+23, 2021.

[24] C. Sullivan, "Protecting digital identity in the cloud: regulating cross border data disclosure," *Computer Law and Security Report*, vol. 30, no. 2, pp. 137–152, 2014.

[25] T. Reynaert, W. De Groef, D. Devriese, L. Desmet, and F. Piessens, "PESAP: A privacy enhanced social application platform," in *Proceedings of the ASE/IEEE International Conference on Privacy, Security, Risk and Trust/ASE/IEEE International Confernece on Social Computing (SocialCom/PASSAT)*, pp. 827–833, Amsterdam, Netherlands, September 2012.

[26] J. Li, S. Shen, X. Sun, and X. Xing, "Identification and classification for risk paths in the context of cross-BorderImportant data flow," *Chinese Journal of Management Science*, vol. 29, pp. 90–99, 2021.

[27] L. Sun, H. Zhang, and C. Fang, "Data security governance in the era of big data: status, challenges, and prospects," *Data Science and Management*, vol. 2, pp. 41–44, 2021.

[28] X. Liu, S. X. Sun, and G. Huang, "Decentralized services computing paradigm for blockchain-based data governance: programmability, interoperability, and intelligence," *Ieee Transactions on Services Computing*, vol. 13, pp. 343–355, 2020.

[29] J. P. Choi, D.-S. Jeon, and B.-C. Kim, "Privacy and personal data collection with information externalities," *Journal of Public Economics*, vol. 173, pp. 113–124, 2019.

[30] J. van Hoboken and R. O. Fathaigh, "Smartphone platforms as privacy regulators," *Computer Law and Security Report*, vol. 41, Article ID 105557, 2021.

[31] W. Liu, S. Long, D. Xie, Y. Liang, and J. Wang, "How to govern the big data discriminatory pricing behavior in the platform service supply chain? An examination with a three-party evolutionary game model," *International Journal of Production Economics*, vol. 231, Article ID 107910, 2021.

[32] R. Alt, C. Militzer-Horstmann, and H.-D. Zimmermann, "Editorial 25/2: electronic markets and privacy," *Electronic Markets*, vol. 25, no. 2, pp. 87–90, 2015.

[33] L. Sun, Y. Rao, L. Wu, X. Zhang, Y. Lan, and A. Nazir, "Fighting false information from propagation process: a survey," *ACM Computing Surveys*, vol. 55, no. 10, pp. 1–38, 2023.

[34] S. Zannettou, M. Sirivianos, J. Blackburn, and N. Kourtellis, "The web of false information: rumors, fake news, hoaxes, clickbait, and various other shenanigans," *Journal of Data and Information Quality*, vol. 11, no. 3, pp. 1–37, 2019.

[35] E. Odlerova and K. Hyllova, "Dissemination of false information in domestic and foreign media," in *Proceedings of the 13th Annual International Scientific Conference on Megatrends and Media- Reality and Media Bubbles*, pp. 255–272, Smolenice, Slovakia, April 2018.

[36] Z. Guo, L. Wang, Y. Wang et al., "Public opinion spamming: a model for content and users on sina Weibo," in *Proceedings of the 10th ACM Conference on Web Science (WebSci)*, pp. 210–214, Amsterdam, Netherlands, May 2018.

[37] A. Puska, L. A. Baroni, M. C. Canal, L. S. G. Piccolo, and R. Pereira, "WhatsApp and false information: a value-oriented evaluation," in *Proceedings of the 19th Brazilian Symposium on Human Factors in Computing Systems (IHC)*, Electrical network, Vitoria, Brazil, October 2020.

[38] X. Yang, Z. Zhou, X. Hao, and Y. Xiao, "Analysis of platform economic supervision mode from the perspective of blockchain," *Mobile Information Systems*, vol. 2022, Article ID 3534220, 13 pages, 2022.

[39] G. Braghini and F. Salvarani, "Effects of hidden OPINION manipulation in microblogging platforms," *Advances in Complex Systems*, vol. 24, no. 5, 2021.

[40] H. Xu, "Risk decision method for DEA cross-efficiency based on variable coefficient," *Statistics and Decisions*, vol. 36, pp. 164–168, 2020.

[41] M. Wang, S. Lian, S. Yin, and H. Dong, "A three-player game model for promoting the diffusion of green technology in manufacturing enterprises from the perspective of supply and demand," *Mathematics*, vol. 8, no. 9, p. 1585, 2020.

[42] P. D. Taylor and L. B. Jonker, "Evolutionary stable strategies and game dynamics," *Mathematical Biosciences*, vol. 40, no. 1-2, pp. 145–156, 1978.

[43] X. Qu and G. Hou, "Governance of platform information security based on tripartite evolutionary game," *Journal of Modern Information*, vol. 40, pp. 114–125, 2020.

[44] Y. Guo, K. Zou, M. Yang, and C. Liu, "Tripartite evolutionary game of multiparty collaborative supervision of personal information security in app: empirical evidence from China," *IEEE Access*, vol. 10, pp. 85429–85441, 2022.

[45] S. Zhang and L. Zhu, "Coregulation supervision strategy of drug enterprises under the government reward and punishment mechanism," *Complexity*, vol. 2021, Article ID 5865299, 16 pages, 2021.

[46] S. Gao, X. Liu, and S. Ling, "Local government's information disclosure during environmental incident: a studyfrom the upper-level governments' intervention perspective," *Journal of Intelligence*, vol. 38, pp. 161–168, 2019.

[47] Y. Zhou and F. Yu, "Reputation detection for information diffusion in social network systems," *Complexity*, vol. 2022, Article ID 5317738, 18 pages, 2022.

[48] D. L. Deephouse, "Media reputation as a strategic resource: an integration of mass communication and resource-based theories," *Journal of Management*, vol. 26, no. 6, pp. 1091–1112, 2000.

[49] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[50] P. Resnick, "Trust among strangers in Internet transactions: empirical analysis of eBay's reputation system," *Economics of the Internet and E Commerce*, 2002.

[51] T. Dong, S. Yin, and N. Zhang, "The interaction mechanism and dynamic evolution of digital green innovation in the integrated green building supply chain," *Systems*, vol. 11, no. 3, p. 122, 2023.

[52] Z. Zhang, "Logic and regulation of blockchain empowering carbon digital security governance," *Journal of Intelligence*, vol. 42, pp. 86–93, 2023.