Innovation Series https://www.innoseries.com

Collaborative Governance of National Defense Infrastructure Driven by Data Fusion Quality: A Four-Party Evolutionary Game Analysis

Xuetao Wang, Yahui Wu*

College of Systems Engineering, National University of Defense Technology, Changsha 410073, Hunan, China

Corresponding Author: Yahui Wu

Abstract: Aiming at the realistic pain points of insufficient coordination of national defense engineering construction subjects, prominent information barriers and difficult release of data value, this paper incorporates data fusion quality and information sharing level as parameters into the game analysis framework, and constructs a four-party evolutionary game model including military, local government, central government and construction enterprises. The research shows that the quality of data fusion and the benefit coefficient of information sharing are the core driving forces for the co-evolution of the whole system. The big data supervision of the central government can significantly slow down the security risks of military data sharing; when the security risk coefficient exceeds the critical value, the army will take the lead in exiting data collaboration, causing the system chain strategy contraction. The validity of the conclusion is verified by numerical simulation, which provides theoretical support for the modernization of big data-enabled defense engineering governance.

Keywords: National defense infrastructure; Four-party evolutionary game; Data fusion quality; Information sharing; Security risk; Collaborative governance

1. Introduction

National defense engineering is the core pillar of national security, but its construction faces problems such as information islands, quality supervision, and cross-departmental coordination costs. Big data and Internet of Things technology enable parties to support accurate and transparent construction decisions through data sharing and multi-source fusion, but problems such as willingness to share, quality of data fusion, and trade-offs between confidentiality risks and benefits hinder digital empowerment.

Evolutionary game theory, which models boundedly rational actors' adaptive strategy adjustment [1], has mature stability criteria and evolutionary stable strategy frameworks [2,3], widely applied in engineering and public governance. Most construction studies use tripartite game models to explore quality supervision among owners, contractors and supervisors [4], with recent work extending to digital twin-enabled oversight [5], regulatory drivers of firms' digital upgrading [6], and smart construction multi-stakeholder collaboration [7]. Nearly all such work focuses on civilian construction, leaving confidentiality-bound defense infrastructure largely underexplored; early defense game research on attack-defense protective planning only offers basic methodological reference [8].

Related work on digital government data sharing incentives [9], construction supply chain data quality [10], privacy-preserving sharing mechanisms [11], project incentive effects on sharing [12], and government data opening rules [13] informs our parameter design, but most treats data sharing as a binary variable, overlooking the continuous nonlinear impacts of data fusion quality. Defense construction research prioritizes technical risk assessment and big data supervision pathways [14,15] without quantifying multi-stakeholder strategic interactions; while military-civilian collaborative innovation and macro digital governance studies [16,17] provide insights, they rarely explore data collaboration in security-constrained construction settings [18]. Domestic research on big data governance factors [19] and military-civil data sharing risk evolution [20] guides our variable weighting and risk constraint design.

This paper aims to fill three key gaps: one is to pay attention to the unique military-civilian coordination and confidentiality rules of national defense engineering; the second is to include the quality of data fusion as a continuous endogenous variable into the income function; the third is to correct the simplified linear risk cost hypothesis and introduce the mitigation effect of nonlinear risk escalation and central supervision. This paper constructs a four-party evolutionary game model that integrates nonlinear security risks and regulatory mitigation effects. Through derivation and simulation, it analyzes how the fusion quality drives the evolution of collaborative governance, identifies the boundary of policy intervention, and provides theoretical support for optimizing data-driven governance of defense engineering.

2. Materials and Methods

2.1 Problem Description and Basic Assumptions

This model focuses on the data collaboration dynamics in the whole process of national defense engineering construction, involving four interdependent stakeholder groups. Its core responsibilities are as follows: As the core end user and the main confidentiality responsible party, the military defines the functional requirements of the project, supervises the quality compliance of the construction, and implements the hierarchical data confidentiality rules at the whole stage. Local governments provide on-site support for project landing, including land allocation, cross-departmental coordination and local administrative approval procedures. The central government is at the macro governance level, deploying cross-party sharing digital platforms, and designing hierarchical incentive and punishment mechanisms to shape decision-making.

Drawing on evolutionary game theory and the practical realities of defense projects, we start from a few basic premises. Assumption 1: all four parties are boundedly rational: they adjust their strategies through learning and trial and error, eventually converging to an evolutionarily stable strategy. Assumption 2: The probability of the military choosing deep data collaboration is x ($0 \le x \le 1$), and conventional collaboration is $1-x$. The probability of local governments choosing active data docking is y ($0 \le y \le 1$), and passive cooperation is $1-y$. The probability of the central government choosing big data supervision is z ($0 \le z \le 1$), and traditional supervision is $1-z$. The probability of construction enterprises choosing digital management is w ($0 \le w \le 1$), and traditional construction is $1-w$. Assumption 3: Data fusion quality is an exogenous parameter determined by overall digital technology level. The number of collaborative participants affects the potential upper limit of fusion quality, and this paper analyzes evolution differences under different levels by running sensitivity analyses. Assumption 4: We model the military's security risk as a nonlinear function of data fusion depth: the cost rises slowly at first, then accelerates as sharing deepens. In addition, we allow central big data supervision to offset a fixed fraction of this risk, with mitigation efficiency k ($0<k<1$). Assumption 5: Special subsidies and precise penalties only take effect under the big data supervision mode.

2.2 Evolutionary Game Model Construction

Combined with practical scenarios, core parameters of the model are defined in Table 1.

Table 1: Definition of Core Model Parameters.

Parameter	Definition
R_1	Basic benefit of the military under conventional collaboration
C_1	System construction cost for military deep data collaboration
ΔR_1	Basic collaborative benefit per participant for the military
L_1	Benchmark security risk coefficient of military data sharing
R_2	Basic benefit of local government under passive cooperation
C_2	System construction cost for active data docking
ΔR_2	Basic collaborative benefit per participant for local government
S_2	Special subsidy for local government active docking
R_3	Basic benefit of central government under traditional supervision
C_3	Platform construction cost for big data supervision
ΔR_3	Basic comprehensive benefit per participant for central government
P	Precise penalty for enterprise violations under big data supervision
R_4	Basic benefit of enterprises under traditional construction
C_4	Digital construction cost for enterprises
ΔR_4	Basic efficiency benefit per participant for enterprises
S_4	Special subsidy for enterprise digital construction
λ	Information sharing benefit coefficient, $\lambda > 0$
β	Data element multiplier effect parameter, $\beta > 1$
ϕ	Information transparency coefficient
ΔF	Accountability loss after compliance risk exposure

Based on parameter settings, expected payoff functions of four stakeholders are constructed respectively. For the military, the expected payoff of deep data collaboration is:

$$U_{11}=R_1-C_1-L_1\theta^2(1-kz)-e^{-\phi\theta}\Delta F+\theta^{\beta}\lambda(y+z+w)\Delta R_1$$

The expected payoff of conventional collaboration is:

$$U_{12}=R_1$$

The average expected payoff is:

$$\overline{U_1}=xU_{11}+(1-x)U_{12}$$

For the local government, the expected payoff of active data docking is:

$$U_{21}=R_2-C_2+zS_2+\theta^{\beta}\lambda(x+z+w)\Delta R_2$$

The expected payoff of passive cooperation is:

$$U_{22}=R_2$$

The average expected payoff is:

$$\overline{U_2}=yU_{21}+(1-y)U_{22}$$

For the central government, the expected payoff of big data supervision is:

$$U_{31}=R_3-C_3-yS_2-wS_4+(1-w)P+\theta^{\beta}\lambda(x+y+w)\Delta R_3$$

The expected payoff of traditional supervision is: The average expected payoff is:

$$\overline{U_3}=zU_{31}+(1-z)U_{32}$$

For the construction enterprise, the expected payoff of digital construction management is:

$$U_{41}=R_4-C_4+zS_4+\theta^{\beta}\lambda(x+y+z)\Delta R_4$$

The expected payoff of traditional construction is:

$$U_{42}=R_4-zP$$

The average expected payoff is:

$$\overline{U_4}=wU_{41}+(1-w)U_{42}$$

According to evolutionary game theory, replication dynamic equations describe the change rate of strategy proportion over time. Four replication dynamic equations are derived as follows:

$$F(x)=x(1-x)\left[\theta^{\beta}\lambda(y+z+w)\Delta R_1-C_1-L_1\theta^2(1-kz)-e^{-\phi\theta}\Delta F\right]$$
$$F(y)=y(1-y)\left[\theta^{\beta}\lambda(x+z+w)\Delta R_2+zS_2-C_2\right]$$
$$F(z)=z(1-z)\left[\theta^{\beta}\lambda(x+y+w)\Delta R_3+(1-w)P-C_3-yS_2-wS_4\right]$$
$$F(w)=w(1-w)\left[\theta^{\beta}\lambda(x+y+z)\Delta R_4+z(S_4+P)-C_4\right]$$

2.3 Equilibrium Stability Analysis Method

The local stability of system equilibrium points is judged by the Jacobian matrix eigenvalue method. By taking first-order partial derivatives of strategy variables for the four replication dynamic equations, a 4-order Jacobian matrix is constructed:

$$J=\begin{bmatrix} \frac{\partial F(x)}{\partial x} & \frac{\partial F(x)}{\partial y} & \frac{\partial F(x)}{\partial z} & \frac{\partial F(x)}{\partial w} \\ \frac{\partial F(y)}{\partial x} & \frac{\partial F(y)}{\partial y} & \frac{\partial F(y)}{\partial z} & \frac{\partial F(y)}{\partial w} \\ \frac{\partial F(z)}{\partial x} & \frac{\partial F(z)}{\partial y} & \frac{\partial F(z)}{\partial z} & \frac{\partial F(z)}{\partial w} \\ \frac{\partial F(w)}{\partial x} & \frac{\partial F(w)}{\partial y} & \frac{\partial F(w)}{\partial z} & \frac{\partial F(w)}{\partial w} \end{bmatrix}$$

For pure strategy equilibrium points with $x,y,z,w\in\{0,1\}$, At a pure strategy equilibrium, the Jacobian matrix is diagonal, so its eigenvalues are simply the diagonal elements. An equilibrium is an ESS provided all eigenvalues have negative real parts.

We identified 16 pure strategy equilibrium points in the system, plus several mixed strategy ones. Solving the replicator equations further showed that the mixed strategy equilibria are always saddle points or unstable foci, implying that the system cannot settle there over time. Therefore, this paper focuses on five typical pure strategy equilibria with practical significance.

2.4 Numerical Simulation Setup

All simulations ran on Python 3.10 with SciPy. We solved replication dynamic equations via fourth-order Runge-Kutta (fixed step=0.1), calibrating parameters against prior evolutionary game work, factor analysis weights, and defense project cost-benefit contexts. The initial share of the positive strategy was fixed at 0.5 for each stakeholder, which we interpret as a moderate willingness to collaborate in the early stage of system development. The exact values are given in Table 2.

Table 2: Benchmark Simulation Parameters.

Parameter	Value	Parameter	Value
θ	0.6	ΔR_1	1.9
λ	0.98	ΔR_2	1.7
β	1.12	ΔR_3	2.6
k	0.6	ΔR_4	1.9
L_1	2.2	C_1	1.3
ϕ	2	C_2	0.8
ΔF	1.5	C_3	1.4
S_2	0.5	C_4	1
S_4	0.7	P	1.2

3. Results

3.1 Benchmark Evolution Results

Under benchmark parameters, the strategy evolution trajectories of four stakeholders are shown in Figure 1.

Figure 1: Strategy Evolution Trajectory of Four Stakeholders Under Benchmark Scenario.

The system finally converges to the steady state of all-agent deep data collaboration, which verifies the evolutionary stability of the full collaborative equilibrium. The evolution process presents two typical characteristics.

Convergence speed heterogeneity: the central government converges the fastest, followed by construction enterprises and local governments, and the military is the slowest. The reason is that the comprehensive income of the central government under the supervision of big data is significantly higher than the cost of platform construction and subsidy, forming a strong strategic transformation momentum; the military bears additional security risks and confidentiality costs, and the release of collaborative benefits depends on the joint participation of other parties, resulting in more prudent decision-making.

The nonlinear path of the military strategy: showing the characteristics of ' first drop and then rise '. In the early stage, due to the low proportion of coordination among all parties, the net income of the military for data coordination alone was negative, resulting in a short decline in the proportion of strategies. As the proportion of other parties ' positive strategies increases, the data-enabled revenue continues to grow, the net synergistic revenue changes from negative to positive, and the driving strategy gradually rebounds and eventually converges to a steady state.

3.2 Sensitivity Analysis of Core Parameters

3.2.1 Impact of Data Fusion Quality

Three comparison scenarios with $\theta=0.2$, and are set to explore the impact of data fusion quality on system evolution, as shown in Figure 2.

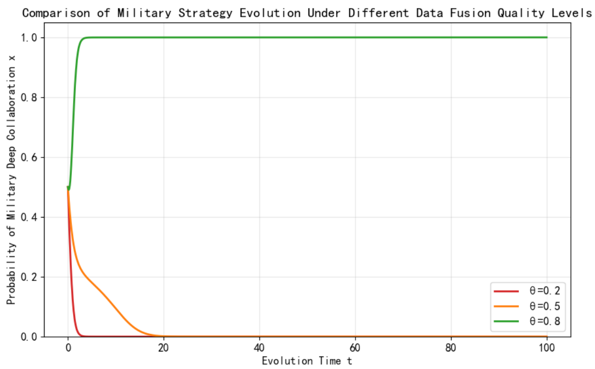

Figure 2: Comparison of military strategy evolution under different data fusion quality levels.

The results indicate that data fusion quality is the primary driver of evolutionary direction, with an obvious critical threshold effect. When $\theta=0.2$, fusion quality is low, the collaborative benefits cannot cover the costs and risks, so the military quickly abandons the positive strategy and the system settles into a low-efficiency state. When $\theta=0.5$, the decline speed slows down, but it still cannot break through the benefit balance point in the long run, and finally converges to zero collaboration. When $\theta=0.8$, We found that high fusion quality greatly amplifies the value of shared data. After a short downward adjustment, the military's strategy share rises and converges to full collaboration. From our parameter sweeps, the critical θ value is around $\theta=0.55$.

3.2.2 Impact of Security Risk Coefficient

Three scenarios with $L_1=0.5$, and are set to verify the constraint effect of security risks, as shown in Figure 3.

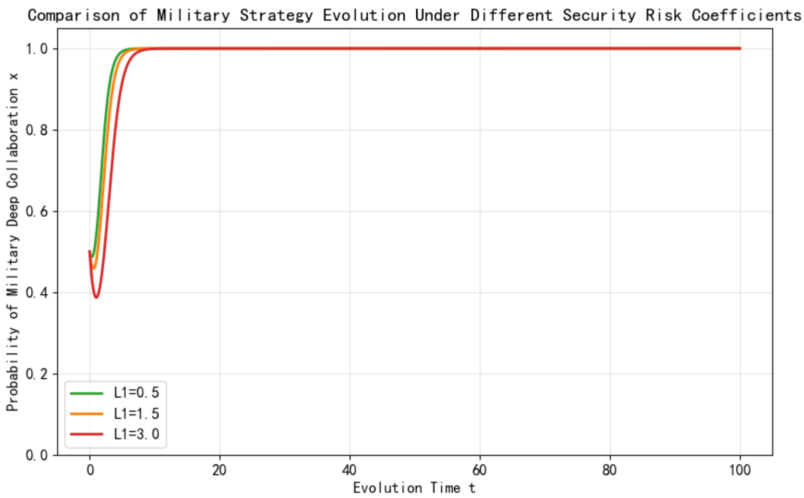

Figure 3: Comparison of military strategy evolution under different security risk coefficients.

All three scenarios finally converge to full collaboration, but the evolution paths show obvious gradient differences. The lower the security risk coefficient, the smaller the initial decline of military strategy and the faster the convergence speed. When L_1=0.5, the risk offset effect is weak, and the strategy converges quickly without obvious decline. When L_1=3.0, risk cost greatly compresses net benefits, and the inflection point of strategy rebound is significantly delayed. If the risk continues to rise above the critical value, the military will eventually withdraw from collaboration, triggering chain degradation of the whole system.

3.3 System Anti-Interference Resilience

In order to measure how the quality of data fusion shapes the resilience of the system, this paper conducts a pulse shock test: after the system converges to the initial steady state, a negative shock of 20 % is applied to the probability of the military choosing deep collaboration. The system resilience under high fusion quality and low fusion quality scenarios is compared, as shown in Figure 4.

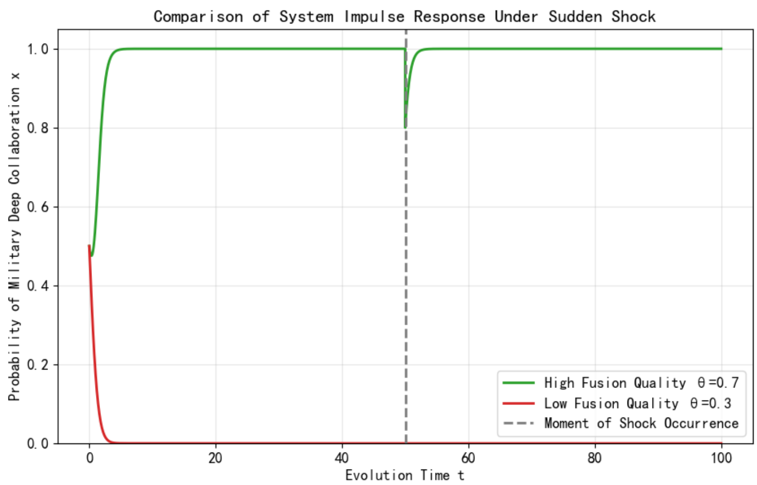

Figure 4: Impulse response comparison of the system under sudden external shock.

The simulation results reveal two very different scenarios.

Low fusion quality: The system cannot lock in stable collaboration, collapses to zero collaboration almost instantaneously, and has little ability to buffer external interference.

High fusion quality: external shocks only cause short-term fluctuations in the level of synergy. Thanks to the self-reinforcing return of high-quality data streams, the system quickly bounces back to full collaborative operation.

The conclusion shows that improving the quality of data fusion not only guides the governance system to the optimal equilibrium, but also significantly enhances the ability of the entire collaborative network to resist accidental interference.

3.4 Supervision Efficiency Parameter Plane Analysis

To quantify the substitution relationship between data fusion quality and penalty intensity, a parameter plane is constructed with system convergence time as the indicator, as shown in Figure 5.

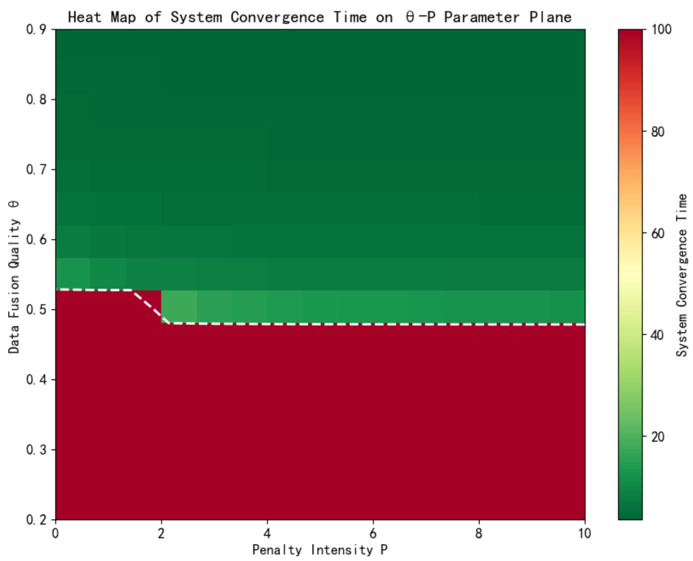

Figure 5: Heat map of system convergence time on θ-P parameter plane.

Three core conclusions can be drawn. First, data fusion quality is the decisive factor for system convergence. When $\theta<0.47$, no matter how high the penalty intensity is, the system cannot converge to full collaboration, and supervision alone is insufficient to overcome the low-efficiency trap. When $\theta>0.52$, the system can converge stably even at low penalty levels. Second, penalty mechanism has a substitution effect in the critical interval. Within $0.47 < \theta < 0.52$,Our simulations indicate that penalties have a limited substitution effect. Each unit increase in penalty intensity lowers the critical data fusion threshold by about 0.03, but only within a narrow range. Once penalty intensity surpasses 3, further increases bring almost no improvement in convergence time; the extra cost of supervision is not justified by efficiency gains.

4. Discussion

4.1 Theoretical Implications

This study applies evolutionary game theory to the field of defense engineering governance under confidentiality constraints, which integrates two defense-specific elements: non-linear security risk cost and multi-level government supervision, and better reflects the reality of military and local governance. Different from the simple ' shared or unshared ' binary framework of previous models, this paper regards the quality of data fusion as a continuous endogenous variable, identifies the threshold effect and bistable effect, and supplements the theory of cross-organizational data collaboration. By introducing impulse response and parameter plane analysis, the framework is extended from static equilibrium to dynamic resilience and policy alternative boundary test, which provides a more intuitive multi-party governance reference than the traditional single-parameter sensitivity analysis.

4.2 Practical Policy Implications

Four targeted optimization suggestions are proposed.

Establish hierarchical data quality certification: formulate unified quality standards and data classification based on confidentiality levels, link quality levels with income and subsidy distribution, and reduce the synergy threshold from the source.

Promote scenario-based full life cycle engineering data reuse. use big data to enable schedule control, defect detection and risk early warning, and enhance the endogenous sharing willingness of stakeholders.

Refined incentive mechanism: provide targeted digital transformation subsidies, implement hierarchical punishment for violations under the supervision of big data, and give priority to improving quality rather than excessive punishment.

Build a central-led technical security system: use privacy computing and federal learning to create an interactive sandbox of ' data availability is not visible ', and alleviate military security concerns through the risk mitigation effect of central supervision.

5. Conclusion

In this paper, the quality of data fusion and the benefit of information sharing are taken as the core parameters, and the four-party evolutionary game model of military, local government, central government and construction enterprises is constructed, and the evolution law and key influencing factors of the system are analyzed. The research mainly draws the following conclusions: First, the data fusion quality and the information sharing revenue coefficient are the core driving forces for the evolution of the system to the fully collaborative optimal state, and the two amplify the collaborative benefits through the multiplier effect. Second, the security risk is a key factor restricting the willingness of military data sharing, and the risk is accelerating with the depth of data fusion. The central government 's big data supervision can effectively mitigate security risks. Thirdly, the policy combination of differentiated subsidies and precise punishment can effectively reduce the cost of subject coordination and accelerate the convergence speed of the system to the optimal equilibrium.

References

[1] Friedman D. Evolutionary games in economics[J]. Econometrica, 1991, 59(3): 637-666.

[2] Weibull J W. Evolutionary Game Theory[M]. Cambridge: MIT Press, 1995.

[3] Hofbauer J, Sigmund K. Evolutionary Games and Population Dynamics[M]. Cambridge: Cambridge University Press, 1998.

[4] Wang H, Li Z, Zhang Y. Tripartite evolutionary game analysis of safety supervision in prefabricated building

construction[J]. Automation in Construction, 2023, 152: 104945.
[5] Liu Y, Chen X, Wang S, et al. Evolutionary game analysis of construction quality supervision under digital twin-enabled supervision mode[J]. Sustainability, 2023, 15(11): 8677.
[6] Zhao L, Sun Z. Digital transformation of construction enterprises: An evolutionary game analysis of government supervision and enterprise adoption[J]. Buildings, 2024, 14(3): 721.
[7] Chen M, Liu H, Zhang Q. Evolutionary game analysis of multi-stakeholder collaboration in smart construction projects[J]. Journal of Construction Engineering and Management, 2024, 150(5): 04024052.
[8] Liu G D, Wang H. Tripartite evolutionary game model of protective engineeringplanning under attack-defense confrontation[J]. Journal of National University of Defense Technology, 2023, 45(2): 187-194.
[9] Gao Y, Li X, Wang Q. Evolutionary game analysis of multi-stakeholder data sharing in digital government[J]. Government Information Quarterly, 2023, 40(2): 101897.
[10] Li Y, Chen L, Wang Q. Data quality investment and sharing strategy in construction supply chains: An evolutionary game perspective[J]. Computers & Industrial Engineering, 2023, 182: 109432.
[11] Xu J, Zhang Y, Li S. Privacy-preserving data sharing in cross-organizational collaboration: An extended evolutionary game approach[J]. Information Sciences, 2024, 654: 119876.
[12] Chen Y T, Zhang B J. Evolutionary game research on incentive mechanism of data sharing in engineering construction[J]. Systems Engineering — Theory & Practice, 2024, 44(1): 156-170.
[13] Zhang B, Chen Y. Incentive mechanisms for government data opening: A comparative analysis based on evolutionary game[J]. Journal of Management Science and Engineering, 2023, 8(4): 521-538.
[14] Zhou L, Wu Y, Luo X. Big data-enabled intelligent supervision in public construction projects: Mechanism and effectiveness evaluation[J]. Automation in Construction, 2024, 158: 105217.
[15] Li X, Wang Y, Zhang Q. Resilience assessment of big data-driven construction governance systems[J]. IEEE Access, 2023, 11: 87654-87665.
[16] Chen Y, Zhang W, Li M. Evolutionary game analysis of military-civilian collaborative innovation in defense technology industrialization[J]. Technological Forecasting and Social Change, 2023, 192: 122587.
[17] Smith J, Johnson R. Digital governance of defense infrastructure: Challenges and collaborative models[J]. Defense & Security Analysis, 2024, 40(2): 189-207.
[18] Wang H, Zhao L. Game analysis of military-civilian data collaboration in defense engineering under security constraints[J]. Defence and Peace Economics, 2024, 35(3): 421-439.
[19] Li G, Liu C. Identification and weight calculation of key influencing factors of big data governance: Based on improved DEMATEL-ANP method[J]. Chinese Journal of Management Science, 2023, 31(8): 215-224.
[20] Wang B Y, Zhang H W. Security risk evolution and governance path of military-civilian integration data sharing in national defense engineering[J]. Journal of Intelligence, 2023, 42(5): 118-126.