Research on Strengthen the Supervision and Administration of Geographic Information Security and Data Governance

Heng Li[1,2]

[1]National Geomatics Center of China, Beijing, China-liheng@ngcc.cn
[2]Technology Innovation Center for Geographic Information Public Service, Ministry of Natual Resources, Beijing, China

Keywords: Geographic information security, Data supervision and administration, Data governance, Data security, Data usage control, Data elements circulation.

Abstract

The advancement of 5G/6G, autonomous driving and the low-altitude economy, together with their derivative technologies, business formats and models, propels the ubiquitous development of surveying and mapping, thus underpinning the progress of intelligent industries. It has become feasible to illegally obtain large-scale, precise location information of ground features quickly in a short period, which poses severe challenges to the supervision and administration of surveying, mapping, and geographic information security. Security be embedded throughout the entire process of geospatial data supply, circulation, and utilization. Firstly, this paper introduces geospatial data security technologies, including the classification and grading of geospatial data and the confidentiality processing of geospatial data, among others. Secondly, a geographic information security supervision and data governance model was designed, which covering geospatial data application scenarios, the geospatial data circulation control model, the geospatial data circulation security architecture and its applications, etc. Finally, the contributions, challenges and opportunities faced by geographic information security supervision and data governance were summarized.

1. INTRODUCTION

As technologies such as intelligent connectivity and artificial intelligence become increasingly mature, and the platform economy evolves at a rapid pace, new products, business formats, and models which including autonomous driving, unmanned driving, and the low-altitude economy are transitioning from pilot demonstrations to application trials, and beginning to enter widespread practical use on a large scale. The advancement of these new technologies, business formats, and models is driving the "ubiquitization" of surveying and mapping. It has become feasible to illegally obtain large-scale, precise location information of ground features quickly in a short period, which poses severe challenges to the supervision and administration of surveying, mapping, and geographic information security. The Surveying and Mapping Law clearly stipulates that "a geographic information security management system and a technical prevention and control system shall be established; supervision and administration of geographic information security shall be strengthened; and traceable management shall be implemented for the acquisition, possession, provision, and utilization of geographic information that constitutes state secrets." Meanwhile, it defines the supervisory responsibilities of the competent authorities for surveying, mapping, and geographic information with regard to satellite navigation and positioning reference stations. Laws such as the Law on Guarding State Secrets and the Cybersecurity Law explicitly require the establishment and improvement of a network-based geographic information security assurance system, as well as the refinement of confidentiality and protection measures. Article 6 of the Data Security Law clarifies that "competent authorities in industries such as natural resources shall undertake the responsibility of supervising data security in their respective industries and fields." The Personal Information Protection Law mandates that sensitive personal information such as location coordinates and movement trajectories shall be protected by law, and competent authorities in industries including natural resources shall be responsible for the protection, supervision, and administration of personal information in their respective industries and fields.

The Opinions of the Central Committee of the Communist Party of China (CPC) and the State Council on Establishing a Fundamental Data System to Better Leverage the Role of Data as a Factor of Production ("Twenty Measures on Data") stipulates: "A trusted data circulation system shall be established to enhance the availability, credibility, circulability, and traceability of data. Dynamic management shall be implemented throughout the entire process of data circulation, and the value of data shall be activated through compliant circulation and utilization." The Opinions of the General Office of the Central Committee of the CPC and the General Office of the State Council on Accelerating the Development and Utilization of Public Data Resources explicitly mandates: "The availability of public data resources shall be improved; efforts shall be made to advance the standardization and regularization of data resources; classified and hierarchical data management shall be carried out; source-level data governance and quality supervision and inspection shall be strengthened; and mechanisms for data quality feedback, traceability of data usage processes, and resolution of data disputes shall be put in place." The Implementation Plan on Improving Security Governance for Data Circulation to Better Promote the Marketization and Valuation of Data as a Factor requires that security be embedded throughout the entire process of data supply, circulation, and utilization. It also mandates making full use of technologies such as trusted data spaces, data circulation controls, data networking, and privacy-preserving computation platforms to establish an efficient, convenient, and trusted data circulation mechanism, thereby facilitating the large-scale, low-cost, secure, and free circulation of data (The CPC Central Committee and The State Council, 2025).

In recent years, incidents involving the illegal acquisition of surveying and mapping data through new technological means such as autonomous driving have occurred frequently. Taking

the whole-process supervision of autonomous driving maps as an example, to strengthen the capacity building of geographic information security supervision and improve the security governance of geospatial data elements, it is necessary to explore and clarify the ownership attribution of surveying and mapping geospatial data generated during the operation, service provision, and road testing of autonomous vehicles. On this basis, research should be conducted on policies and systems related to the ownership relationships of autonomous driving map data and data development and utilization, so as to promote the sharing and utilization of autonomous driving map data.

This paper first introduces geospatial data security technologies, including the classification and grading of geospatial data and the confidentiality processing of geospatial data, among others. Secondly, it designs a geographic information security supervision and data governance model, covering geospatial data application scenarios, the geospatial data circulation control model, the geospatial data circulation security architecture and its applications, etc. Finally, it summarizes the contributions, challenges and opportunities faced by geographic information security supervision and data governance.

2. RELATED WORK

The research on the supervision and administration of geographic information security and data governance is still in its infancy.

In the academic community, Academician Deren Li proposed PNTRC (Positioning, Navigation, Timing, Remote Sensing, and Communication Integrated Space-Based Information Real-Time Service System), with Spatio-Temporal Intelligence Science as its theoretical basis. This system emphasizes the realization of full spatio-temporal perception, cognition, and intelligent decision-making of natural and human activities through intelligent sensors for Communication, Navigation, and Remote Sensing, cloud computing, and artificial intelligence methods (Li et al., 2015; Li et al., 2020). Academician Jiayao Wang put forward the strategic assertion that "independent and controllable basic software is the lifeline of geographic information security." In response to the security challenges in emerging fields such as smart cities and autonomous driving, he further proposed an integrated innovation paradigm of "spatiotemporal intelligence + security" (Wang et al., 2017). However, it lacks elements related to the supervision of geographic information security and data governance.

In the engineering and industry field, The research focuses on the theories, technologies, and applications of geographic information security, and has achieved systematic breakthroughs in fields such as digital watermarking, security control, and confidentiality processing. However, their research achievements can only restrict the copyright attributes of geographic information and the flow of geographic information within single-domain systems, and fail to address the challenges of full-lifecycle secure circulation and supervision of cross-domain geospatial data.

3. KEY TECHNOLOGIES FOR GEOGRAPHIC INFORMATION SECURITY SUPERVISION

Currently, research on geographic information security supervision and data governance in academic and industrial circles is still in the initial stage. Geospatial data circulation refers to the process of geospatial data transmission among different entities, which usually includes methods such as opening, sharing, transaction and exchange. The basic model of data circulation (Li et al., 2025) is shown in Figure 1, which depicts the process of exchange and transfer of geographic information resources between data providers and data demanders.

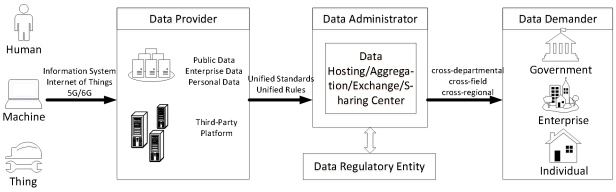

Figure 1. The Basic Model of Data Circulation.

3.1 Geographic Information Security Supervision

Researchers usually adopt single or combined technical means such as digital watermarking, data encryption, access control, confidentiality processing, and blockchain to ensure the security of geospatial data at different protection levels, preventing the leakage, theft, and tampering of geographic information.

3.1.1 Digital Watermarking: refers to a technology that embeds hidden identification information (i.e., digital watermarks) into geospatial data (such as vector data, raster data, and 3D data) to protect the copyright of geospatial data, verify data integrity, and track data leakage or tampering. Among them, vector map data watermarking is usually divided into different implementation methods based on technical principles, including robust watermarking, fragile watermarking, reversible watermarking, asymmetric watermarking, plug-in visual watermarking, and spliced watermark detection. In contrast, remote sensing image watermarking is relatively simple, mainly consisting of two technical routes: robust watermarking and semi-fragile watermarking.

3.1.2 Access Control: through spatial attribute fusion, dynamic policy decision-making, and multi-level security models, it provides refined permission management for geospatial data. Based on user identity, attributes, environmental conditions, or spatial location, it dynamically grants or denies access rights to prevent unauthorized operations (such as illegal downloading, tampering, or unauthorized analysis).

3.1.3 Confidentiality Processing: also known as desensitization technology for geographic information, it involves desensitizing geographic information by deleting information such as key targets, key elements, and key attributes, as well as reducing coordinate accuracy and altering graphic similarity, according to characteristics such as the representation elements, element attributes, and data accuracy of geographic information. Common technical methods include coordinate transformation processing based on affine transformation, coordinate transformation processing based on map projection, and information processing based on deleting key targets.

3.2 Geospatial Data Governance

Data governance is a process that aims to improve data quality, security, and compliance, and promote the effective utilization of data. It includes organizational data governance, industry data governance, social data governance, and data security governance, among others. geospatial data governance mainly involves core links such as geospatial data classification and grading, and geospatial data security protection.

3.2.1 Classification and Grading of Geospatial Data: the classification and grading of geospatial data is a prerequisite for the confirmation of rights, authorized use, compliant, efficient, and trustworthy circulation and utilization of geospatial data, as well as the safe governance of element circulation. Currently, geospatial data is classified and graded in accordance with relevant policy documents and standards, such as Information Security Technology - Requirements for Classification and Grading of Network Data, Measures for Data Security Management in the Field of Natural Resources, and Guidelines for the Classification and Grading Management of Government Affairs Data of the Ministry of Natural Resources. Specifically, geospatial data resources mainly include categories such as fundamental geospatial data, remote sensing image data, and thematic geospatial data. Based on factors such as the importance, accuracy, scale, depth, currency, and security risks of geospatial data, it is divided into three levels: general, important, and core.

3.2.2 Geospatial Data Security: with the development and application of technologies such as blockchain and privacy-preserving computation, geospatial data protection has integrated these new technologies and methods, leading to a series of innovative geospatial data protection means. For example, blockchain smart contracts are used to automatically execute geospatial data desensitization rules and record geospatial data usage logs; differential privacy methods that add controlled noise to geospatial data to ensure the usability of calculation results while preventing identification of specific individuals; and quantum-secure encryption and federated learning to protect the transmission and storage security of geospatial data.

4. DESIGN AND CONSTRUCTION OF GEOSPATIAL DATA SECURITY SUPERVISION AND DATA GOVERNANCE MECHANISM

Based on the research of cross-domain geospatial data, the basic model of geographic information security supervision and data governance mechanism was proposed (Li et al., 2023; Li et al., 2024; Li et al., 2025). The design and implementation of the supervision and data governance model for geographic information security mainly encompasses aspects such as the application scenarios of geospatial data, the geospatial data circulation control model, and the security architecture for geospatial data circulation and its applications.

4.1 Application Scenarios of Geospatial Data

With the wide application of remote sensing images featuring high temporal, high spatial, and high spectral resolution, as well as surveying and mapping remote sensing technologies, in fields such as the "Unified Map" for territorial spatial planning and natural resources management, Realistic 3D China, global geographic information resources, and marine surveying and mapping, the importance of controlling the circulation and utilization of geospatial data in scenarios like exchange, opening-up, and sharing has become increasingly prominent. The whole-process management of geospatial data which including its collection, release, processing, utilization, storage, and destruction relies mainly on the real-time intelligent service network for aerospace information integrated with Communication, Navigation, and Remote Sensing (referred to as the PNTRC Network for short).

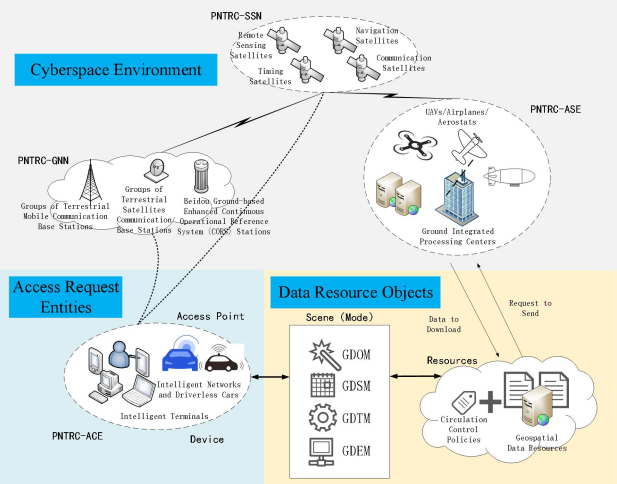

Figure 2. The PNTRC Network Scene of Geospatial Data Circulation.

PNTRC as a composite network architecture that integrates communication satellite systems, navigation satellite systems, remote sensing satellite systems, and the Beidou satellite navigation system-supported Ground-Based Augmentation Continuous Operational Reference System (CORS). Its core design aims to achieve the goals of "one satellite for multiple uses, multi-satellite networking, multi-network integration, and intelligent services," while realizing in-depth coupling between the "space-based network" and "ground-based network." Relying on this integrated structure, PNTRC can, in accordance with user requirements, transmit corresponding geographic information and communication data in real time to user-end devices which including mobile phones, intelligent connected vehicles, mobile terminals, computer network equipment, and communication base stations. This capability further enables it to meet the intelligent service demands in various application scenarios involving the circulation and utilization of geospatial data, as shown in Figure 2.

4.2 Geospatial Data Circulation Control Model

To address emerging challenges brought by new information service models and dissemination methods in ubiquitous cyberspace such as the separation of data ownership and management rights, and secondary/multiple information circulation Li Fenghua et al. proposed a Cyberspace-oriented Access Control (CoAC) model. This model consists of three components: access request entities, networks/generalized networks, and resources (sets). Its essence lies in associating access control for network access with authorization/authentication of information systems. By integrating real-time context awareness, fine-grained access control, and lifecycle data usage management, the model achieves fine-grained control in ubiquitous access scenarios, thereby ensuring the secure and flexible management of sensitive data across organizational boundaries. Our research team developed the Geospatial Data Circulation Control (GDCC) model (Li et al., 2026) based on the CoAC model, which includes the base model and its administration model, as shown in Figure 3.

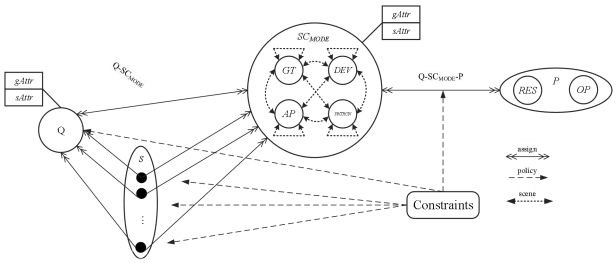

Figure 3. The Geospatial Data Circulation Control (GDCC) Base Model.

4.2.1 Access Request Entities: geospatial data circulation access request entities Q (Quantity) include users (ordinary users, administrator users) and sessions. Among them, access users consist of geospatial data providers, users, and supervisors; a session refers to the process of accessing geospatial data resources through clients, including basic services such as navigation, timing, remote sensing, and communication, as well as services of upper-layer application businesses.

4.2.2 Cyberspace Environment: The cyberspace environment for geospatial data circulation includes general temporal, access points, access devices, PNTRC networks, and other elements, as shown in Table 1.

Elements	Connotation of Element
General Temporal (GT)	It refers to the dynamic association of multi-dimensional date, time, and other related information when a geospatial data resource access request is triggered.
Access Point (AP)	It refers to the Cyberspace Resources Surveying and Mapping Space Location (CRSMSL) or Network Identity (NetID) where the access request entity for geospatial data circulation first accesses the PNTRC network with a route hop count of 1, through cyberspace resource surveying and mapping.
Device (DEV)	It refers to the equipment used for accessing geospatial data circulation resources in the PNTRC network, mainly including mobile phones, intelligent connected vehicle sensors, mobile terminals (handheld RTK/GPS measuring instruments, Beidou navigators, etc.), tablet computers, laptops, desktop computers, servers, CORS reference station receivers, space-based satellite network terminals, space-based satellite network ground terminals, Ka-band high-capacity broadband terminals, Ku-band (FDMA/TDMA) terminals, etc.
PNTRC Network (PNTRCN)	It is the carrier for geospatial data transmission and the collection of all information transmission channels, including space-based satellite networks, ground-based node networks, application server networks, and application client networks.

Table 1. The Cyberspace Environment for Geospatial Data Circulation of the GDCC Model.

4.2.3 Data Resource Objects: Data resource objects for geospatial data circulation include resources, scenes, and other elements, as shown in Table 2.

Elements	Connotation of Element
Resource (RES)	It refers to the objects accessed by access request entities in the geospatial data circulation under the complex PNTRC network environment, including management data, current status data, and application data. Among them, management data includes monitoring data, status data, application data, broadcast data, etc.; current status data includes fundamental geospatial data, electronic map data, remote sensing image data, 3D real-scene data, underground pipeline data, etc.; application data can be divided into forward data and return data according to the flow direction, and into position coordinates, spatiotemporal data, high-precision maps, etc., according to the content.
Scene (SC)	It refers to the element conditions required for an access request entity to initiate a session and obtain permissions when accessing data resources in the complex PNTRC network.

Table 2. The Data Resource Objects for Geospatial Data Circulation of the GDCC Model.

The PNTRC-oriented geospatial data Circulation Control (GDCC) model includes the mapping of all elements such as geospatial data resource access request entities, general temporal, access points, resources (operations), access devices, networks, and scenes (circulation modes) on CoAC. Taking operations in resource mapping as an example: operations in the geospatial data circulation environment refer to the access actions of access request entities on geospatial data resources such as vector data, raster data, and 3D data in the PNTRC network, and the authorization for geospatial data circulation and usage is realized through the continuous execution of these actions. According to the type of application data resources, operation types can be divided into Positioning Navigation Timing Operation (PNTO), Remote Sensing and Monitoring Operation (RSMO), Autonomous Driving Operation (ADO), Communication and Transmission Operation (CTO), etc., with one operation type corresponding to multiple allowed operations.

Taking the circulation mode in scene mapping as an example: Circulation Mode (MODE) refers to the methods adopted by access request entities for accessing data resources in the PNTRC network. According to the corresponding goals of the scene, it can be divided into Geospatial Data Open Mode (GDOM), Geospatial Data Sharing Mode (GDSM), Geospatial Data Trading Mode (GDTM), Geospatial Data Exchange Mode (GDEM), etc. The relevant goals of geospatial data circulation and usage are achieved through the above method types. Under different scene circulation modes, there are differences in the geospatial data circulation and usage control scenarios and their management.

Within the complex network environment of PNTRC, the management model for geospatial data circulation and utilization control mainly comprises the following modules: Scene Administration (SCAD) for attribute scenarios (circulation modes), Scene and Privilege Administration (SCPAD) for attribute scenarios (circulation modes), User and Scene Administration (USCAD) for user-attribute scenarios (circulation modes), User Identity Management (note: the original text cites "USCAD" here, which may be a notation

consistency issue; standard nomenclature would align with domain conventions if revised), and Session Management (SM).

4.3 Security Architecture for Geospatial Data Circulation and Its Applications

We propose a security architecture for geospatial data circulation and its applications (Li et al., 2024; Li et al., 2026). The proposed architecture supports the efficient and secure transmission and execution of control strategies, thereby ensuring that geospatial data is protected against unauthorized access and tampering during the circulation process, as shown in Figure 4.

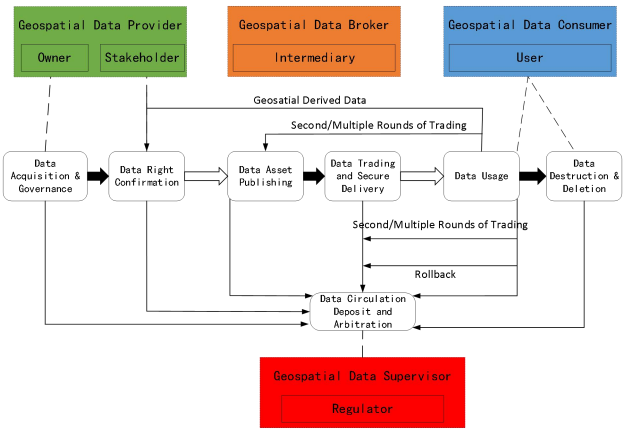

Figure 4. The Security Architecture for Geospatial Data Circulation and Its Applications.

4.3.1 Key Links of Geospatial Data Circulation: including collection and governance, data right confirmation, data asset release, data transaction and secure delivery, data usage, data destruction and deletion, circulation certification and arbitration, as shown in Table 3.

Key Links	Connotation of Key Links
Collection and Governance	It refers to the operations performed by data holders on geospatial data, such as cleaning, classification and grading, and metadata management, to facilitate subsequent data circulation and utilization.
Data Right Confirmation	It is the process by which authoritative institutions determine the ownership of geospatial data. In the event of disputes over data ownership and rights and interests, interested parties can resolve the disputes through arbitration..
Data Asset Release	It involves publishing the confirmed geospatial data assets on trading platforms to facilitate the transaction of data elements.
Data Transaction and Secure Delivery	It means that relevant parties in the geospatial data transaction negotiate transaction contracts in accordance with the wishes of the transacting parties, and deliver the data to the data user accurately, completely and in a timely manner in accordance with the contracts.
Data Usage	It refers to the processing and utilization of geospatial data by data users in accordance with the contract terms to realize data value-added. Data usage shall ensure that usage control is implemented in accordance with contract constraints throughout the entire circulation process.
Data Destruction and Deletion	It refers to the destruction and deletion of geospatial data in accordance with contracts or the requirements of data owners after the data has achieved its intended use.
Circulation Certification and Arbitration	It involves realizing certification throughout the entire circulation process of geospatial data elements, and interested parties can resolve disputes through arbitration in the event of conflicts.

Table 3. The Key Links of Geospatial Data Circulation.

4.3.2 Geographic Information Security Supervision Under Different Circulation Scenarios: including geospatial data openning, sharing, trading and exchange scenarios, etc.

In the scenario of open sharing of geospatial data, within the context of open sharing of geospatial data, national-level nodes and provincial-level nodes of public geographic information services are required to share registered user information and published geospatial asset data. Given that the geospatial asset data that has been formed and published is made public and available for free use, it only requires focus on geospatial data security governance and does not involve issues related to geographic information security supervision.

In the scenario of geospatial data exchange, the exchange of geospatial asset data, products, and services primarily takes place in the forms of "one-to-one" and "point-to-point" interactions, involving data types such as spatiotemporal big data and realistic 3D data. Within this scenario, the focus is primarily on the application of encryption technologies in the transmission encryption and storage encryption links of geospatial information data assets. This application aims to achieve transmission control, storage integrity, and confidentiality protection for important or core geospatial data.

In the scenario of geospatial data transaction, on-exchange and off-exchange transactions are conducted primarily through "one-to-many" or "many-to-many" models, which mainly realize the transaction and circulation of geospatial asset data, products, and services in the form of concluded contracts.
Therefore, the security architecture for geospatial data circulation can be effectively applied to links such as data transaction and secure delivery, data utilization, as well as data destruction and deletion.

5. CONCLUSIONS AND CHALLENGES

Currently, there is a paucity of research on security supervision and data governance in the context of the circulation of geospatial data elements. Based on the cyberspace-oriented access control model, we proposed the Geospatial Data Circulation Control Model, as well as a trusted verification method for control strategies based on timed automata. Meanwhile, aiming at the problems of efficient transmission and secure storage-access of control strategies and circulating data in the scenario where massive geospatial data undergoes frequent cross-domain circulation in complex network environments, we put forward an efficient and secure execution mechanism for geospatial data circulation control strategies. This mechanism enables the compliant, efficient, and controlled utilization of geospatial data throughout its full circulation

lifecycle, thereby providing theoretical and application support for the circulation of geospatial data elements.

On the one hand, there is insufficient capacity to address potential risks brought by new technologies and new business formats. Research on the security risks arising from the application of new technologies such as autonomous driving and intelligent connectivity is inadequate, and there is a lack of regulatory measures for new business formats. Faced with new technology models and the influx of massive data, it is urgent to break through new technologies, develop new tools, and enhance the "proactive prediction" capacity of surveying, mapping, and geographic information supervision. On the other hand, security prevention and control are weak. The network security level protection grades of various regulatory systems are inconsistent, equipment is insufficient, the guarantee capacity of commercial cryptography application needs to be improved, and the protection capacity is difficult to meet the requirements.

5.1 Overall Planning for Capacity Building

Focus on prominent issues such as insufficient capacity to address potential risks brought by new technologies and new business formats, insufficient overall coordination and integration, and weak security prevention and control. In accordance with the Overall Plan for Improving the Digital Governance Capacity of Natural Resources, carry out overall construction from three aspects: the construction of regulatory application scenarios for new business formats and traditional surveying, mapping, and geographic information, environment establishment and system integration, and the collection and management of regulatory data. Promote the research and development of geographic information security supervision means adapting to the development of new technologies and new business formats.

5.2 Focus on Core Businesses

Facing the development trend of new technologies and new business formats, focus on government regulatory responsibilities, promote the unified construction of network infrastructure and hardware environment, unified management of regulatory data, integrated application of regulatory functions, and collaborative intelligence of regulatory capabilities, so as to realize full-process, full-coverage and traceable supervision of surveying, mapping, and geographic information.

5.3 Embrace Artificial Intelligence

Facing new artificial intelligence (AI) technologies and applications, with the innovative breakthroughs in generative AI technology, large models have been increasingly widely applied in everyone ’ s life, study, and work. In particular, the emergence of DeepSeek has greatly reduced the technical threshold for large model deployment. For geographic information security supervision and data governance, it is necessary to clarify the application scenarios of large models, standardize deployment models, define operation and management requirements, and formulate safeguard measures.

ACKNOWLEDGEMENTS

The work was sponsored by National Geomatics Center of China (NGCC) Innovation Fund.

REFERENCES

Li, D., Ma, J., Shao, Z., 2015: On Spatiotemporal Big Data and Its Applications. *Satellite Application*, 09:7-11.

Li, D., Shen, X., 2020: Research on the Development Strategy of RealTime and Intelligent Space-Based Information Service System in China. *Strategic Study of Chinese Academy of Engineering*, 22(02):138-143.

Li, F., Li, H., Niu, B., et al., 2024: Research Category and Future Development Trend of Data Elements Circulation and Security. *Journal on Communications*, 45(05):1-11. https://doi.org/10.11959/j.issn.1000-436x.2024106.

Li, H., Huang, W., Xu, Y., et al., 2025: Research on Strengthen the Development and Utilization of Geospatial Data to Release the Value of Data Elements. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, Volume XLVIII-G-2025, Pages 913-919, 6-11 April 2025.

Li, H., Huang, W., Zhao, W., et al., 2023: Research on Geographic Information Data Circulation Supports the Construction of Digital China. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, Volume XLVIII-1/W2-2023, Pages 97-104, 2-7 September 2023.

Li, H., Huang, W., Zhai, Y., et al., 2024: Research on New Spatial Data Infrastructure Supports the Circulation of Geographic Information Data Elements. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, Volume XLVIII-4-2024, Pages 303-309, 22-25 October 2024.

Li, H., Li, F., Guo, Y., et al., 2026: Circulation Control Model and Administration for Geospatial Data. *Lecture Notes in Computer Science*, Volume 16217 LNCS, Pages 525-544, 2026. https://doi.org/10.1007/978-981-95-3540-8_28.

Li, H., Li, F., Liang, W., et al., 2025: Modeling and Verification of Data Circulation Control Based on Timed Automata. *Journal on Communications*, 46(03):13-27. https://doi.org/10.11959/j.issn.1000-436x.2025038.

Li, H., Li, F., Shi, X., et al., 2025: Research on Access Control for Secure Cross-domain Data Circulation. *Journal on Communications*, 46(04):238-254. https://doi.org/10.11959/j.issn.1000-436x.2025042.

The CPC Central Committee and The State Council, Notice Issued by the National Development and Reform Commission and Other Relevant Departments on the Implementation Plan for Improving the Security Governance of Data Circulation and Better Promoting the Marketization and Valuation of Data Elements.https://www.gov.cn/zhengce/zhengceku/202501/content_6998668.htm (24 Oct 2025).

Wang, J., Wu, F., Guo, J. Z., et al., 2017: Challenges and Opportunities of Spatio-temporal Big Data. *Science of Surveying and Mapping*, 42(07):1-7. https://doi.org/10.16251/j.cnki.1009-2307.2017.07.001.