ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-202308.00225

A Review of India's Data Localization Paradigm and Its Implications for China (Post-Print)

Authors: Fan Ying

Date: 2023-08-23T00:00:00+00:00

Abstract

Data localization is a focal issue in global data governance, and its impact on global data governance is no longer confined to a single country or region. For many years, India has followed a unique policy framework regarding cross-border data flows and data localization, and its insistence on data sovereignty also reflects its position on the international stage. This article takes India's data localization paradigm as its research foundation to discuss the widespread phenomenon of a disconnect between the policy motivations and actual effects of data localization, and uses this as an entry point to introduce India's latest research findings in this field. As an effective approach for developing countries to address data security, data localization measures—through a paradigmatic study of India's data localization—reveal that this disconnect between policy motivations and actual effects is both a common problem and involves structural irrationalities in framework construction and limitations in research methodologies; adjusting the current governance framework for localization can help alleviate the tension between data internationalization and regulatory localization. Moreover, reasonable rules for cross-border data flows should seek a balance between the values of security and development. China is both an advocate and an important promoter of economic globalization; actively participating in the formulation of international rules for cross-border data flows and enhancing its discourse power in cross-border data governance will be China's normative choice.

Full Text

Citation Format

Fan Y. Paradigm Review of Data Localization in India and Its Implications for China. *Bulletin of Chinese Academy of Sciences*, 2023, 38(8): 1177-1186, doi: 10.16418/j.issn.1000-3045.20230318001. (in Chinese)

Title

Paradigm Review of Data Localization in India and Its Implications for China

Author Affiliation

School of Law, Henan University of Economics and Law, Zhengzhou 450046, China

Abstract

Data localization is a focal issue in global data governance, and its impact extends far beyond national borders. For years, India has followed a unique policy framework regarding cross-border data flows and data localization, with its insistence on data sovereignty reflecting its position on the international stage. This article uses the Indian data localization paradigm as a research foundation to discuss the common phenomenon of disconnect between policy motivations and actual effects of data localization, and introduces the latest research findings in this area from India. As an effective approach for developing countries to address data security, the paradigm study of India's data localization reveals that this disconnect is not only a shared problem but also stems from unreasonable framework construction and methodological limitations in research. Adjusting the current governance framework for localization can help alleviate tensions between data internationalization and regulatory localization. Moreover, reasonable rules for cross-border data flows should seek a value balance between security and development. As both an advocate and important promoter of economic globalization, China should actively participate in international rule-making for cross-border data flows and enhance its discourse power in cross-border data governance.

Keywords: Data Localization, Data Protection, Data Regulation, India

1 India's Data Localization Policy Background and Position

India is a beneficiary of the digital economy era. Digital trade enhances productivity by connecting Indian businesses with world-class digital goods and services, thereby reducing the costs for India's micro, small, and medium enterprises to participate in international trade and broadly benefiting the Indian economy. India possesses a vast talent pool of approximately 1.5 million engineers and scientists and over 9,300 technology startups. In 2021-2022, India's IT services exports exceeded $150 billion for the first time, making the IT industry a leading sector in India with a prominent position in the international division of labor. Indian companies are providing ed-tech, fintech, and health-tech services to global customers, attracting the attention of multinational corporations—some of which have already invested in India (such as Facebook and Google) while others have shown considerable interest. India's success is attributed to

favorable public policies both domestically and from foreign trade partners, including open market access for India's digital service exports.

However, as the digital economy expands, the Indian government has expressed four major concerns about the free flow of data: (1) storing data on foreign servers objectively hinders Indian security agencies' access to such data; (2) economic losses caused by foreign companies' misuse of data; (3) concerns about foreign surveillance; and (4) violations of privacy rights through misuse of personal data. These concerns have formed a consensus across various sectors in India: data flows must be regulated. Although existing academic research tends to focus on digital trade liberalization and the necessity of cross-border data flows, such research is currently insufficient to unravel the complex regulatory dilemmas associated with data localization.

In 2019, India had a population exceeding 1.2 billion and 627 million internet users, making it one of the largest data-generating countries. Recognizing the critical role of data in economic development, the Indian government has initiated measures and policies such as the 2018 Reserve Bank of India (RBI) Payment Directive, the 2019 Draft National e-Commerce Policy, and the 2020 Non-Personal Data Governance Framework to achieve data localization and data protection. These policies involve certain restrictions on data flows, with some also addressing the development of local data infrastructure in India through enhanced domestic manufacturing capabilities.

In the debate between data localization and data free flow, India maintains an independent position. At global forums, India has shown reluctance to participate in negotiations related to data flows, data protection, and data localization. For example, India has not joined the WTO e-commerce negotiation group and refused to sign the Osaka Declaration on the Digital Economy, which attempted to have countries discuss cross-border data free flow outside the WTO framework. India also withdrew from RCEP negotiations, citing among other reasons that the agreement introduced prohibitive norms on data localization. While establishing a framework for securely generating, collecting, and exchanging data at the global or regional level would better leverage the potential of data and the digital economy, India has chosen temporary "non-cooperation" to continue building a robust domestic data regulatory system. Indian Commerce and Industry Minister Piyush Goyal stated that the digital divide within and between countries severely hinders developing countries from benefiting from digital trade. Like other developing countries, India needs time and policy space to deeply understand negotiation topics and develop its own legal and regulatory frameworks before engaging in e-commerce negotiations.

2 Important Measures of India's Data Localization: The Personal Data Protection Bill and RBI Payment Directive

India has implemented varying degrees of localization measures, both cross-sectoral and sector-specific. For instance, the 1993 Indian Public Records Act

prohibits transferring public records outside India without prior government approval, unless such transfer is for official purposes. The government's "GI Cloud National Private Cloud Program" (also known as "MeghRaj") aims to promote government use of cloud services and includes requirements for government data localization. Under this program, a basic condition for cloud service provider selection is that data center facilities and physical and virtual hardware must be located within India. The 2000 Information Technology Act and the 2011 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (hereinafter "IT Rules") prohibit corporate bodies from transferring sensitive personal data outside India unless the other party achieves the same level of data protection as stipulated in the IT Rules. Additionally, there are sector-specific localization requirements. For example, licensing agreements between telecom service providers (TSPs) and the Indian government prohibit licensees from transferring any subscriber information and accounting data to any person or place outside India, except for international roaming or billing purposes. In contrast, India's Companies Act regarding maintenance of company accounting records is relatively lenient, only requiring that backups of company books and other documents maintained in electronic form be regularly stored on servers physically located in India.

2.1 Four Iterations of India's Personal Data Protection Bill

In August 2017, India's Ministry of Electronics and Information Technology established an expert committee chaired by former Supreme Court Justice Srikrishna (hereinafter "Srikrishna Committee") to examine issues related to data protection in India and formulate a Personal Data Protection Bill. In July 2018, the committee released the proposed Personal Data Protection Bill (Draft) 2018, which the Indian government subsequently published for public comment. The draft combined data localization and data sovereignty, expanding the scope of the Personal Data Protection Bill to data fiduciaries outside India through explicit localization requirements in certain cases.

The Srikrishna Committee proposed a "three-pronged" approach to regulate cross-border transfers, categorizing the processing of personal data and critical personal data. It recommended storing at least one live, working copy of personal data in India. Critical personal data designated by the government would be subject to stricter constraints, permitted to be stored and processed only in India. The government has the authority to exempt certain data from cross-border flow regulations based on national strategic interests. However, under the draft, this exemption does not apply to sensitive personal data.

Data localization became one of the most controversial topics in the Personal Data Protection Bill, with disputes existing not only among stakeholders but even among committee members. After more than a year of preparation, the Indian government introduced a revised draft, the Personal Data Protection Bill (Draft) 2019. The 2019 revised draft proposed a significantly relaxed cross-border data flow framework, eliminating general restrictions on personal data

transfers and replacing them with mirror requirements for sensitive personal data and mandatory local storage and processing requirements for critical personal data. Notably, the revised draft still did not define the concept of critical personal data but allowed the Indian government to designate certain personal data as critical, granting the government extensive power to store, use, and control large amounts of data, which sparked considerable 质疑 and criticism both domestically and internationally. After more than two years of deliberation and one withdrawal, the Indian government released the Digital Personal Data Protection Bill (Draft) 2022 (hereinafter "DPDP Draft") on November 18, 2022. The DPDP Draft does not explicitly mention data localization requirements; regarding cross-border transfers of personal data, the Indian government will notify data fiduciaries to transfer personal data to countries or regions outside India according to prescribed terms and conditions after evaluating necessary factors. Currently, this approach appears extremely similar to adequacy requirements under the GDPR, with future details of personal data cross-border transfers depending on specific conditions determined by the Indian government's adequacy assessments; if these conditions are too stringent, they will still produce de facto data localization effects.

2.2 RBI Payment Directive

On April 6, 2018, the Reserve Bank of India (RBI) issued a payment directive requiring all payment system-related data to be stored locally in India. The directive mandates that all system providers ensure complete data related to their payment systems is stored only in systems located in India. This requirement extends to all intermediaries and third-party vendors processing data on behalf of payment system providers. The only exception involves cross-border transactions—if necessary, data related to overseas branches of transactions may be stored abroad. The directive initially granted operators a six-month compliance grace period, requiring submission of compliance reports to the RBI by October 15, 2018. The primary objective is to ensure Indian regulatory authorities have unrestricted access to payment data for supervision. Additionally, before issuing the directive, the RBI mentioned the need to adopt global best practices for data security and protection to reduce data breach risks.

According to media reports, up to 80% of industry participants, including Amazon, Alibaba, and WhatsApp, have complied with the payment directive. Visa has become one of the first global financial services companies to comply with the RBI payment directive, paving the way for greater market share in India. Meanwhile, Visa's competitors, including Mastercard and American Express, were ordered to stop onboarding new users for non-compliance with the payment directive.

In April 2021, the RBI further tightened its compliance norms, requiring all licensed payment system operators (PSOs) to submit detailed compliance certificates twice a year by April 30 and October 31. The compliance certificate must be signed by the CEO or managing director to confirm that the system

operator complies with all RBI regulations regarding secure storage of payment data. This clearly exceeds the one-time compliance report requirement in the April 2018 payment directive. It is speculated that this move is related to a series of cybersecurity breaches experienced by Indian tech startups; the rationale being that if sensitive data is stored on specific servers that facilitate regulation, cyberattacks would be limited.

However, the payment directive appears not to consider the fact that most financial entities maintain their data in encrypted form, and the RBI itself requires banks and other payment entities to use 128-bit encryption for online communications. Consequently, encrypted data remains illegible without assistance from relevant payment entities. Given that storing all payment data in India aims to achieve unrestricted regulatory access, the payment directive fails to consider that regulators must still require payment entities to decrypt data according to statutory procedures to achieve access. Therefore, mandatory data localization alone is insufficient to achieve the stated regulatory objectives.

3 Policy Motivations and Evaluation of India's Data Localization

The proliferation of data localization measures is closely associated with the strong rise of the digital economy. In the absence of any global compact to unify internet architecture, states' assertions of sovereignty in cyberspace have become international consensus—a position that has existed since the internet's inception. In this context, data localization is one of a series of measures aimed at implementing national control over digital ecosystems. Examining policy objectives helps assess what data localization can and cannot achieve in reaching its goals, most importantly identifying the actual problems data localization seeks to solve and the feasibility of alternative measures. Simultaneously, to reduce unnecessary trade friction, it is essential to fully consider the international impact of adopting data localization and how to respond.

Although numerous arguments support or oppose data localization, whether it can achieve its stated objectives is an important research starting point. The following four objectives are explicitly elaborated in multiple Indian government documents: (1) ensuring law enforcement access to personal data; (2) preventing foreign surveillance; (3) stimulating economic growth; and (4) better enforcing data protection laws and regulations. The following sections will combine India's current legislation and recent domestic research findings to develop these arguments.

3.1 Ensuring Law Enforcement Access to Data

Law enforcement access to data typically involves three considerations: (1) crime prevention. Access to encrypted data can help law enforcement monitor potential criminals to prevent crimes; furthermore, monitoring suspects' social media accounts and financial transaction activities helps law enforcement track ter-

rorism financing and prevent attacks. (2) criminal investigation. Faster data access helps law enforcement conduct investigations more quickly. For example, access to GPS data helps locate criminal suspects, while broader access to financial data assists in investigating various money laundering activities. (3) economic objectives. Access to existing datasets of foreign enterprises can help Indian companies enhance competitive advantages in fields like artificial intelligence (AI) and create more jobs for Indians.

In practice, law enforcement frequently encounters situations where the data they seek was collected in India but stored in another jurisdiction. While Mutual Legal Assistance Treaties (MLATs) can facilitate access to personal data, the process is cumbersome, taking an average of about ten months. Moreover, even if foreign enterprises store data in India, they remain subject to their home country's laws; data localization and data access are not truly equivalent.

Meanwhile, due to limited access rights to certain data held overseas, particularly content data, Indian law enforcement faces serious constraints. Under current Indian laws, law enforcement first requires enterprises to provide relevant personal information; second, whether the enterprise possesses such information is crucial; most importantly, even if the enterprise possesses such information, whether it has the right to provide it to Indian law enforcement. U.S. enterprises currently hold most of the world's personal data, making them the primary counterpart for data access. Since the U.S. Electronic Communications Privacy Act provides an exception allowing U.S. enterprises to voluntarily provide non-content data to Indian law enforcement, this means U.S. enterprises will cooperate with Indian law enforcement requests for non-content data regardless of whether India adopts localization measures. If Indian law enforcement requests content data, it must still go through the MLAT process, taking about ten months. Due to U.S. domestic law, localization measures will not significantly improve data access from the United States. When data is controlled by non-U.S. enterprises, existing evidence cannot confirm that data access scope and timing differ based on localization measures. Combined with MLAT inefficiency, localization is unlikely to be the best strategy for improving law enforcement data access; maintaining the status quo is clearly suboptimal. For Indian law enforcement, the best alternative to localization is signing bilateral agreements with countries that restrict access to such data, including fixing broken procedures under existing mutual legal assistance treaties and other bilateral or multilateral arrangements to enable data sharing and exchange between nations.

3.2 Stimulating Economic Growth

Analysis from the Global Trade and Innovation Policy Alliance indicates that keeping Indian consumers' data within India will better promote India's economic growth and support innovation compared to free data flow. Supporting arguments include that localization increases local demand for data storage services and provides Indian companies with competitive advantages—if this holds

true, then stricter data localization policies would be more beneficial for India's economic growth. Currently, local demand for data storage services in India is growing daily, but it is difficult to determine to what extent this growth is driven by anticipated localization measures.

(1) Data localization will certainly stimulate demand for building data centers in India but may not necessarily drive GDP growth. India is one of the world's largest data consumers, with its market size expected to double within five years. At least part of this data storage demand will be met locally, and localization measures provide important impetus for this demand. A recent study by an Indian research institution shows that although India has comparative advantages in producing certain products needed for data center construction, imports of data center equipment have grown far faster than exports in recent years. Moreover, India's overall trade balance has continued to deteriorate over the years, with very little domestic value-added in such imported products for India. If products needed for data center construction rely on imports, this demand increases the GDP of the importing country rather than India's GDP. Therefore, while domestic demand for infrastructure drives GDP growth, the overall impact on GDP growth also depends on whether this demand is ultimately met through domestic production or foreign imports.

(2) Mandatory implementation of data localization in India affects not only foreign companies but also Indian companies. Foreign companies must bear the costs of data storage and processing in India, and the recurring costs of leasing or operating data center infrastructure in India are typically higher than foreign companies' existing costs. These increased cost consequences also directly or indirectly affect Indian companies currently storing consumer data outside India. Furthermore, while improved data availability may bring some economic benefits, sharing personal data requires other supporting policy measures, and even with all these measures in place, it remains unclear whether data localization is a necessary condition for implementing them.

3.3 Preventing Foreign Surveillance

Since preventing foreign surveillance is a legitimate objective of every sovereign state, data localization requirements are often considered justified. Storing data within India somewhat restricts foreign ability to access data, but given the complexity of current intelligence collection strategies and analytical methods, geographic location of data cannot be a sufficient barrier against foreign intelligence threats. Moreover, the United States has created legal avenues for its government to access data stored overseas by U.S. companies through the CLOUD Act. To fully protect domestic data from such interference requires a degree of isolation from the internet, which is undesirable and impractical in modern society.

3.4 Better Enforcement of Data Protection Laws and Regulations

Regarding enforcement of India's domestic data protection laws and regulations, alternative methods to localization have been found, namely requiring foreign enterprises to establish local subsidiaries or branches to ensure domestic legal compliance. For example, financial entities processing payment business cannot provide services in India without RBI authorization, which in turn requires them to register as Indian entities. Thus, enforcement of data protection laws depends on whether foreign enterprises establish commercial presence in India, not on data localization requirements. Meanwhile, data localization cannot advance jurisdictional claims or reduce jurisdictional conflicts. This requirement for foreign enterprises to establish local commercial presence also provides a basis for extraterritorial exercise of jurisdiction.

4 Implications for China

India's burgeoning economy has entered a highlight moment of digital economic development. In 2020, India's digital economy value-added reached $541.9 billion, ranking 8th globally and making it one of only two developing countries in the top eight economies. As a developing economy, India's digital trade development shares considerable homogeneity with China: both have established huge domestic markets and numerous internet users, and both have been committed to improving domestic data security regulatory systems in recent years. While India's insistence on data sovereignty determines its position on the international stage, its emerging regulatory system and current academic research remain worthy of reference.

4.1 Correctly Identifying Specific Problems Data Localization Seeks to Solve

Correct problem identification is the starting point for policy intervention and the basis for evaluating various solutions. Current research on data localization often uses domestic policy motivations as a starting point, lacking identification of specific problems. Motivations such as stimulating economic growth and preventing foreign surveillance are somewhat broad and do not clarify the specific problems data localization itself seeks to address. Without common standards and substantial empirical research, using policy motivations as arguments is clearly insufficient to support data localization legislation. Data localization, appearing in a defensive posture, is attributed more protectionist elements due to the ambiguity of its policy objectives. Therefore, correctly identifying problems also constitutes a prerequisite argument for data localization.

According to Article 37 of China's Cybersecurity Law, "operators of critical information infrastructure shall store personal information and important data collected and generated during operations within the territory of the People's Republic of China in China." Important infrastructure in key industries and sectors, once damaged, functionally lost, or experiencing data leaks, would se-

riously endanger national security, national economy, people's livelihood, or public interests. Therefore, the main policy basis behind China's data localization measures is cybersecurity. However, the law does not further define specific circumstances that endanger cybersecurity or what degree constitutes serious concern for cybersecurity, nor does it authorize relevant departments to further interpret security and specific circumstances of threats.

4.2 Evaluating Alternative Solutions to Problems

After specific problems are identified, the next logical step is to evaluate all alternative solutions to the problem and their relative costs and benefits. The evaluation aims to determine whether data localization can become the least intrusive mechanism to solve current problems through Occam's Razor of public policy, and how closely the measure approaches the harm to be prevented. The evaluation should incorporate factors including the impact of proposed measures on civil liberties, national operations, and economic impacts on all stakeholders. For example, regarding enforcement of India's domestic data protection laws, alternative solutions already exist—requiring foreign enterprises to establish subsidiaries or branches in India rather than requiring enterprises to build data infrastructure in India. In this case, enforcement depends on whether foreign enterprises establish commercial presence, not on data localization requirements. Meanwhile, data localization cannot advance jurisdictional requirements or reduce jurisdictional conflicts. This approach of requiring foreign enterprises to establish local commercial presence also provides a basis for extraterritorial exercise of jurisdiction.

When data localization is temporarily irreplaceable, establishing corresponding evaluation criteria with appropriate weights facilitates regulators' choice among multiple data localization schemes. The evaluation criteria should be built around urgent problems to be solved and potential risks. For example, when foreign enterprises must build data centers locally, besides considering whether the scheme has necessary connections to the problem to be solved, consideration must also be given to risks of foreign enterprises exiting, risks of foreign retaliation against domestic overseas companies, and risks of reciprocity-based "de-Sinicization." Different weights should be applied based on different problems to be solved for comprehensive evaluation. Among existing localization schemes, the least intrusive measures should be prioritized. For example, requiring near real-time reporting or data mirroring for certain types of data can ensure the same level of regulatory access. It is recommended to only turn to the strictest localization form—storage and processing only within the territory—when the above schemes cannot achieve established regulatory objectives.

4.3 Designing Inclusive Exception Clauses to Ensure Regulatory Authority and Liberalization

In China, data security has been elevated to the level of national security. The primary responsibility of the Cyberspace Administration of China, the agency in

charge of data regulation, is not to promote industry development but to maintain cybersecurity. It is precisely this pursuit of security that has given rise to data regulatory policies such as restricting cross-border data flows, mandatory data localization, and source code transfer. However, reasonable rules for cross-border data flows should seek a value balance between trade, security, and development. Data localization, as a territorial regulatory model that strictly restricts cross-border data flows, applies traditional territorial sovereignty concepts to the global modern digital economy, easily creating conflicts between security and development. As both a beneficiary and important promoter of economic globalization, and with cross-border data flows being an important component of digital economic globalization, China should actively participate in international rule-making for cross-border data flows and enhance its institutional power in global digital governance.

When designing a comprehensive digital framework to address various data-related social, economic, security, and protection issues, China should combine its own specific needs and objectives, continuously improve its domestic data regulatory system while actively participating in international rule-making for cross-border data flows. Currently, from the negotiating positions of WTO Joint Statement Initiative participants to rules promoted by bilateral and regional trade agreements, a basic position and practice of prohibiting data localization has been formed. From a legislative coordination perspective, designing inclusive exception clauses can reduce risks of domestic regulation facing external challenges. Regarding data localization measures, it is essential to carefully assess their impact as trade policies on the domestic economy, and on this basis rigorously design reasonable security, industrial, and privacy exceptions to dynamically meet current digital economic development needs without being overly constrained by international obligations in trade agreements.

5 Conclusion

Data localization is a focal issue in global data governance, and its impact on global data governance is no longer confined to a single country. A country's regulatory position on data in trade agreements is often influenced by its domestic paradigm, and India is no exception. India's insistence on data sovereignty reflects its position on the international stage. In the digital trade domain, India hopes to follow its own policy framework regarding cross-border data flows, data localization, and privacy protection rather than promoting this process through bilateral or multilateral trade agreements. This strategy is inadvisable in the era of digital economic globalization, but India's current domestic research on data localization rules remains worthy of reference. Since the international digital ecosystem revolves around the most developed economies, data security issues in developing countries are often neglected. As a developing economy, facing the absence of a global governance framework for cross-border data flows, the question of whether to resist pressure and further improve domestic data regulatory systems or actively participate in international rule-making for cross-border data

flows to secure institutional power in global digital governance—India provides a paradigm reference for us.

References

1. Bailey R, Parsheera S. Data localisation India: Questioning the Means and Ends. New Delhi: NIPFP, 2018.
2. Chander A, Lê U P. Breaking the Web: Data Localization vs. the Global Internet. California: California International Law Center, 2014.
3. Observer Research Foundation. India-US Data Sharing For Law Enforcement: Blueprint for Reforms. Washington DC: ORF, 2019.
4. Global Trade and Innovation Policy Alliance: Economic Implications of Cross-Border Data Flows. Washington DC: GTIPA, 2019.
5. National Assocation of Software and Service Companies. Indian Tech Start-up Ecosystem—Leading Tech in 20s. Uttar Pradesh: NASSCOM, 2019.
6. Indian Market Research Bureau. Digital Adoption and Usage Trends. Mumbai: IMRB, 2019.
7. Department of Electronics and Information Technology. Request for Proposal for Provisional Empanelment of Cloud Service Providers. New Delhi: DeITY, 2015.
8. Chander A, Lê U P. Breaking the Web: Data Localization vs. the Global Internet. California International Law Journal, 2015, 64(3): 677-739.
9. Mukherjee A, Sinha S, Sarma A, et al. COVID-19, Data Localisation, and G20: Challenges, Opportunities and Strategies for India. New Delhi: ICRIER, 2020.
10. China Academy of Information and Communications. Global digital economy white paper—A new dawn of recovery from the shock of the epidemic. Beijing: CAICT, 2021. (in Chinese)
11. Zhang W. Enlightenment from the analysis of the 2020 edition of the Classified Disciplines and Majors in America. Academic Degrees and Graduate Education, 2020, 37(1): 59-64. (in Chinese)
12. Xu D Q. The construction of trade rule framework that governs cross-border data flows. Administrative Law Review, 2022, (4): 50-60. (in Chinese)

Author Biography

FAN Ying is an Associate Professor at the School of Law, Henan University of Economics and Law. Her main research areas include international trade law and digital trade governance. E-mail: fanny106@163.com

Responsible Editor: Yue Lingsheng

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv — Machine translation. Verify with original.