MINDWELL SCIENCE PRESS SDN. BHD.

Journal of Emerging Technology Governance
Volume 1, Issue 1

RESEARCH ARTICLE

Global Governance and Domestic Challenges: A Study of the Pluralist Path of India's Cybersecurity Strategy

Shujun Zhang[1,*]

[1] *Teaching and Research Office of World Economics and Politics, Party School of the Jiangsu Provincial Committee of the Communist Party of China, Nanjing 210000, Jiangsu, China*

*** Corresponding author:** Shujun Zhang, E-mail: zhangshujun@jsdx.gov.cn

Published: 28 June 2026

Abstract

India's cybersecurity strategy presents a pluralist path under the influence of both global governance and domestic challenges. Beginning with the evolution of India's information technology policy, this article shows how pluralist considerations arising from historical competition and from choices made in international strategy form the basis of that strategy. It then analyses how domestic factors—the mismatch between India's will and its capacity, the pressure of international governance, and great-power competition—have shaped the strategy's adjustment. Finally, focusing on data security in the course of digitalisation, it sets out the opportunities and challenges India faces in "data nationalism", in international cooperation, and in building its integrated artificial intelligence and data platform. Confronted with an insufficient capacity to respond to cyber threats and with high-end technological innovation that remains inadequate, India seeks to strengthen its cybersecurity protection system through policy, legislation and technological deployment, and to secure room for flexible strategy within international competition and cooperation.

Keywords: India, pluralism, cybersecurity, artificial intelligence, data security

1 Introduction

"Once cities were built along rivers; today, highways run beside them. In the future they will be built on fibre-optic networks and new infrastructure." After resolving to advance the vision of "Digital India", Prime Minister Modi looked forward, in this poetic manner, to the blueprint of India's future development and shared it with India and with the world.

As a country that achieved informatisation relatively early, India has consistently taken a comparatively cautious and incremental approach to formulating cybersecurity strategy, and the formation of that strategy is closely bound up with its foreign strategy: while responding to domestic development, India has continually adjusted its tactics, gradually forming a cybersecurity strategy with Indian characteristics. Overall, India's cybersecurity strategy presents a pluralist path, evident at two levels. At the domestic level, it takes policy, law and multi-stakeholder governance as its instruments, attaching particular importance to the data security involved in the course of digitalisation. At the international level, when confronting such structural tensions as the absence of international governance rules and the cyber hegemony of the great powers, it advocates common governance through pluralist cooperation.

Research on India's cybersecurity strategy is currently concentrated in the following areas. The first is the state of India's cybersecurity industry, examining the provision of security technology and services within India's cyberspace sector[1]. The second is cybersecurity law and policy, focusing on the current state of and the difficulties confronting India's legislation against online violence[2]. The third is international cooperation and its challenges, in particular studies of the current state and prospects of cooperation between Japan and India in cyberspace under the framework of the Indo-Pacific strategy, which bring out the process, logic and challenges of international cooperation in cybersecurity governance[3]. The fourth is the cybersecurity relationship between the United States and India, approached mainly from the two directions of US–India cybersecurity competition[4] and cooperation[5], analysing the external transformation, endogenous drivers and proliferation of contradictions in that cooperation. The fifth is an overview of India's capacity-building in cyberspace, including technological development and policy formulation[6], together with India's participation in the international governance of cyberspace[7]. The sixth concerns data localisation and the construction of a cybersecurity system, a newly prominent field of focus, covering the difficulties and opportunities encountered by India's data localisation policy[8] and the construction of India's cybersecurity system[9].

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Research in China on India's cybersecurity has currently displayed three trends. First, the perspective has moved from within outward, extending from attention to India's own cybersecurity industry to cooperation and competition with the world's major countries. Second, the dimensions of research have become richer, attending not only to capacity-building at the technological level but also to the formulation and implementation of law, policy and strategy. Third, the field of research has continued to expand, turning from the single issue of cybersecurity to comprehensive analysis across multiple fields and levels, encompassing the economic, political and social. Overall, however, Chinese research has mostly concentrated on theoretical analysis, lacking deep excavation of actual cases and empirical study, and the data used in some studies cannot reflect the most recent research progress. At the same time, there is relatively little comparative research on cybersecurity between India and other countries, which limits any comprehensive assessment of the effectiveness of its strategy.

Research in the field of Indian cybersecurity is progressively deepening, and close attention needs to be paid to the structural contradictions and strategic pressures India faces at home and abroad. Indeed, India's international strategic choice has already shifted from the traditional "non-alignment" towards "multi-alignment". The key question that follows is whether India's overall strategic turn will be projected onto, and affect, its cybersecurity strategy. Because of India's deficiencies in core cybersecurity capacity and in high-end technological innovation, together with the mismatch between the government's will and its actual capacity and its underestimation of the complexity of cybersecurity and of domestic political challenges, its government has continually adjusted its choices in cybersecurity strategy, tending in the end towards a pluralist path. It is from this standpoint, combining the practice and the theory of India's cybersecurity governance, that this article seeks, building on existing research, to explore further the logic of formation, the characteristics of evolution and the practical implications of India's cybersecurity strategy.

2 The Cornerstone of India's Cybersecurity Strategy

As a global base for software outsourcing, India's information technology "miracle" was once renowned internationally. Since the Modi government proposed "Digital India", legislation and regulation have been continually issued and refined in order to respond to a rapidly evolving cyber environment at home and abroad. It is worth noting that the post-colonial historical legacy has shown two faces in shaping India's internet ecology. Facing a turbulent international strategic situation, India has advanced steadily in the field of cybersecurity and has spoken up actively in the formulation of cybersecurity governance rules, seeking to secure the greatest possible benefit for itself.

2.1 The Information Technology Miracle and "Digital India"

In 2010 *The Economist* voiced its admiration for India's "economic miracle". The "miracle" derived from the rapid development of India's indigenous information technology industry in the 1980s, when the household workshop economy was gradually displaced by a modern corporate economy. Information technology entrepreneurs, who had brought advanced technology and a global vision back from the West, became the spokesmen and opinion leaders of India's "new economy" and drove a transformation in the country's mode of governance. Thanks to this solid foundation in information technology, the Fourth Industrial Revolution found fertile soil in India. The once world-renowned "information technology miracle" and India's existing information technology base supplied the world's primary information technology market with an enormous quantity of primary technical talent.

India's internet users have become the second largest body of registered users and users of social media in the world, after the United States, and young people flock to new technology and to a technological way of life. According to World Health Organization statistics, India's demographic structure shows a trend towards youth, with those under 35 having become the main component of Indian society. Where the world's major developed countries and emerging economies generally face the predicament of an ageing population, India's enormous demographic dividend has been and will continue to be one of the core competitive factors in its contest for cybersecurity governance.

India's information technology industry, established in the 1960s, took off suddenly in the 1980s, and its average annual growth rate of 30 per cent has made a considerable contribution to the Indian economy. India's information technology industry provides services to more than 580 institutions in 75 countries[11], and the market value of Tata Consultancy Services in that year surpassed that of such globally renowned internet enterprises as Facebook, Baidu and LinkedIn. How did this economic miracle come about in India? One view has become mainstream: the development of the information technology industry exceeded the traditional scope of Indian government regulation, and in the early period there was not even relevant law to regulate it. This therefore gave early internet companies room for almost "savage growth" and enabled them to profit on the basis of extremely low labour costs. As early as 2000 the Indian Minister of Information Technology said bluntly that "the reason India has been able to become a leader in the field of information technology is that the government has not set foot in this field"[12].

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

After Prime Minister Modi came to power, "Digital India", proposed from the standpoint of national strategy, initiated efforts at governing internet space. India's Ministry of Electronics and Information Technology has said that "Digital India" will transform India into a country sustained by a "digital society and knowledge economy". Although the strategy has been much questioned since it was issued and implemented, the global COVID-19 pandemic imperceptibly gave it a new impetus and new opportunities at home and abroad. In content, "Digital India" involves multiple dimensions of domestic and foreign policy and is continually being expanded, comprising the following key elements: first, creating "digital infrastructure", establishing a lifelong digital identity for the people and providing secure and reliable network access; second, "government and services", providing the public with real-time services online and via mobile devices and achieving seamless digital connection between governments or jurisdictions at every level; third, "digital empowerment of citizens", enabling citizens to gain comprehensive access to digital resources and the corresponding digital rights.

Since "Digital India" was proposed, the Indian government has vigorously advanced cybersecurity and digital information technology education, established governmental bodies of various kinds, continually formulated and refined relevant laws and regulations, and encouraged private enterprise to develop in the internet field. The issuance of India's cybersecurity strategy policy documents has undergone the repeated trials of proposal, refinement, revision, return and final promulgation, and is still in the process of being refined. Among these, the policy framework consists mainly of the *National Cyber Security Policy* promulgated in 2013 and the portions of India's Twelfth Five-Year Plan concerning cybersecurity. The *Draft Encryption Policy* released in 2015 was withdrawn two days after publication because its stringent provisions provoked public protest. The *Information Technology Act* promulgated in 2000 is India's important statute for dealing with technology and cybersecurity, and the *Information Technology Act, 2008* (Amendment) is an important supplement to the 2000 version, coming into effect the following year after its passage by the Indian Parliament. The participants in governance are, first, government departments: the Prime Minister's Office established the National Cyber Security Coordinator's Office in 2015 and set up the National Cyber Security Research Fund. India's Ministry of Electronics and Information Technology is the core department of the Indian government for cybersecurity governance and bears the principal governmental responsibility. The Ministry of Home Affairs is responsible for India's domestic cybersecurity, while the Ministry of Defence is traditionally the department responsible for India's international cybersecurity. The Institute for Defence Studies and Analyses (IDSA) and the Defence Research and Development Organisation (DRDO) under the Ministry of Defence are mainly engaged in research on cybersecurity and national security. The participation of industry bodies in cybersecurity governance is a distinctive feature of India's cybersecurity governance, the best known of them being the Data Security Council of India (DSCI), a data protection company established by the National Association of Software and Service Companies (NASSCOM). In addition, civil society organisations, think tanks, and academic institutions of both a technical and a non-technical character all take an active part in India's cybersecurity governance, each playing a positive role[4].

A review of the formation of India's cybersecurity institutions and mechanisms shows that, proceeding from the multiple standpoints of policy, law and multi-stakeholder governance, and through policy leadership, legal constraint and multi-stakeholder participation, India has gradually explored and established its own framework of cybersecurity strategy. The historical legacy of colonialism and an increasingly taut international strategic environment have together accelerated, from within and from without, the formulation and implementation of India's cybersecurity strategy. As India continues to expand in the cyber domain, how to balance the multiple pressures at home and abroad and further refine and consolidate its pluralist strategic path has become the core issue of India's future cybersecurity governance.

2.2 The Trauma of History and Choices in International Strategy

The post-colonial historical legacy has had a profound influence on the development of science and technology and of cybersecurity in India. Nehru, writing in his *Glimpses of World History* of his feelings towards the British, observed that "in one sense, the British have done India a great service. The vigorous life of the English people gave the whole of India a tremendous shock, and also brought to India a sense of nationhood. A new class educated in English began to appear… they were destined to take the leading position in the national movement"[13]. It was precisely this group, educated in frontier technology in the West, that in the post-colonial context played, on the one hand, a key role in technical education and business and, on the other, shaped through discursive forms and media representation the core features of the contemporary Indian internet ecology. While the internet has driven India's social development, it has also brought negative effects: the Mumbai terrorist attacks and interference in elections, among others, are all closely bound up with internet communication.

The relative neglect of India by the outside world provided it with a relatively relaxed environment for development. When the world's attention was mainly concentrated on such cyber powers as the United States, China and Russia, India's development in cyberspace instead gained new opportunities. Similar to the "ungoverned" rapid expansion of India's domestic information technology at the outset, India likewise faced relatively few external constraints and little intervention in international competition. Through its technical experts of Indian origin and its nationals in the management of

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

international organisations, India secured more benefits for itself in the formulation of cybersecurity governance rules. In October 2014 India proposed that the International Telecommunication Union (ITU) should lead and discharge the function of internet governance, in an attempt to bring internet governance back within an intergovernmental pluralist framework rather than leaving it mainly in the hands of the technical bodies led by the United States. This conception of cybersecurity pluralism is entirely of a piece with the guiding principles of India's foreign strategy.

3 The Adjustment of India's Cybersecurity Strategy

As the global security situation has continued to tighten, India's foreign strategy has gradually shifted from "non-alignment" to "multi-alignment", and it displays an evident hedging intent within the pattern of Sino-American strategic competition. Overall, India's framework of cybersecurity strategy is relatively complete, but at the domestic level it still faces a marked gap between the government's will and its actual capacity, while at the international level it encounters the multiple challenges of structural tension. India therefore had few early options in cybersecurity strategy, and instead adjusted continually through tactical vacillation, without rashly adopting an aggressive hedging strategy. This approach is consistent with the great-power strategic objective established at India's founding and is bound up with the interweaving of multiple domestic and external factors.

3.1 The Domestic Predicament: Will and Capacity

The cybersecurity problem is first of all an internal issue of sovereignty and governance. The formulation of cybersecurity strategy must proceed from the country's actual circumstances, delimit the security baseline within the manpower, material resources and financial resources it can bear, and then coordinate this with international participation, so as finally to establish a cybersecurity strategy suited to national conditions. However grand the strategic conception, the concrete challenges are extremely practical.

For the Indian government, the most prominent difficulties can be summarised in the following respects. First, the pace of infrastructure renewal is too slow: where new infrastructure is being advanced throughout the world, India still appears unable to "catch up". Second, cybersecurity education is lacking and its effectiveness is far from adequate, evident not only at the governmental level, since enterprises and individuals likewise lack sufficient publicity and training. Third, the capacity to maintain cybersecurity is weak, and there is a shortage of means of response matched to the current cybersecurity situation, so that external forces can readily penetrate India's domestic networks, with the result that cybersecurity incidents occur frequently in India. Fourth, there is a lack of effective coordination among India's various cybersecurity actors. The organisation of cybersecurity governance within the government is confused, with overlapping functions and insufficient coordination; the military services each go their own way, and the integration of military and civilian actors is difficult to advance; the private sector mostly relies on self-management. Although India was the twelfth country in the world to pass a cybersecurity law, the refinement of its national cybersecurity strategy remains slow.

Although India started relatively early in the field of information technology, its subsequent momentum for innovation has consistently been insufficient. Rather than attributing this to a national character of "resting content with the status quo", it is more accurate to say that the complexity of India's domestic political system and social environment is the more critical constraint. First, the identity of "low-end service provider" has long afflicted the development of India's network technology industry. India's software services sector is strongly oriented towards outsourcing, and most software enterprises within the country act only as subcontractors within the global network system, undertaking offshore or project-level secondary subcontracting. Second, the high-quality development of India's network information technology struggles forward for want of government policy endorsement, and in the mastery and application of high-end information technology India lags behind the global mainstream. A report of the Data Security Council of India (DSCI) proposes that India's cybersecurity industry should achieve a growth target of 35 billion US dollars (approximately 234.5 billion yuan) in output value by 2025, will continue to promote the development of cybersecurity start-ups, and will carry out research and development projects with government support, covering such fields as encryption, cryptanalysis, steganography, network and system security assurance, network monitoring, network forensics and capacity-building. Third, nationalist tendencies are extending from traditional physical space into cyberspace. Because the control and storage of data involve such multiple issues as national security, public morality, public order, personal privacy, consumer rights, domestic law enforcement and industrial development, the concept of "data nationalism" has accordingly emerged [14]. The Indian government emphasises the importance of data localisation and advocates effective restraint of the opening and abuse of data in order to safeguard national data security, and this has also become the projection onto the international level of India's domestic cybersecurity governance.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

3.2 The International Predicament: Structural Tension

The structural tension confronting global cybersecurity governance derives mainly from the absence of a universally applicable and binding international legal framework to regulate the conduct of states in cyberspace. The treaty most widely recognised at present is the *Budapest Convention*, and India is not a signatory to it.

1. Divergence over data access and cross-border enforcement. India and the Western countries differ markedly on the question of cross-border data access. Taking cross-border data enforcement as an example, India mainly relies on mutual legal assistance treaties (MLATs) to obtain the information it needs. To date India has signed such treaties with 42 countries, six of which incorporate the relevant content of international conventions in their provisions. By contrast, the United States has amended federal law through the *CLOUD Act*, granting US government agencies the power to access data controlled by service providers within the United States irrespective of where the data are stored, and at the same time allowing the US government to conclude executive agreements with other countries so that the relevant service providers may share data directly. Because the *CLOUD Act* lowers the threshold for data access, it has attracted severe criticism.

The *Budapest Convention* is at present the legal basis most often cited internationally for dealing with disputes over data access. The Convention emphasises the principle of mutual legal assistance and establishes a supplementary cooperation mechanism for states that have already concluded mutual legal assistance treaties. In only two specific situations does it permit a party to obtain data unilaterally without the authorisation of the other party: first, data that are publicly available; second, data accessed on a computer system within the territory of one party while stored elsewhere, but only with the "voluntary consent" of the lawful holder of the data. The European Union is likewise actively promoting legislation on an electronic evidence mechanism, so as to provide a uniform legal basis for the cross-border access to data by the law enforcement agencies of member states. For example, the draft report submitted in November 2019 by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament substantially revised the proposal, clarifying further obligations on service providers and emphasising the protection of fundamental rights. The draft, however, awaits further deliberation and approval.

2. Disputes over notification and enforcement. At the level of enforcement in cross-border data matters, the rights of states and of the individuals concerned to be notified of a request are also much disputed. Because their fields of application differ, the various legal instruments differ in their safeguards and in their scope of protection. For example, although the draft second additional protocol to the *Budapest Convention* leaves room for notifying another party, this is not a mandatory provision; and the European Union's electronic evidence proposal requires notification to the other party only where "a data request may affect immunities and privileges or otherwise prejudice the fundamental interests" of that party. To address such limitations, the draft report of the LIBE Committee proposed an "automatic notification mechanism", but this still requires further study before it can be put into effect. By contrast, the draft second additional protocol to the *Budapest Convention* provides mainly that "specific procedural instructions" may be set out in an order, including a prohibition on notifying the user or other third parties, so as to prevent information from leaking. Stakeholders generally call, however, for law enforcement to be required to give notice to individuals and for gag orders to be permitted to be delayed only in specific circumstances, with such delay subject to approval through a judicial process.

Because India is not a signatory to the *Budapest Convention*, it cannot take part in the negotiation and formulation of the second additional protocol; by the same token, the European Union's internal legislation on electronic evidence does not apply to India. Yet, once more and more countries accede to these agreements, they will inevitably have an indirect effect on India's future strategy in cyberspace.

3. The absence of international law and the problem of cybercrime. International law further lacks a unified legal framework for dealing with grave incidents in cyberspace. States usually cooperate through Interpol or through bilateral and multilateral mutual legal assistance treaties, and an effective global consensus is difficult to form. Traditional international law continues to play only a limited guiding role with respect to cybercrime: although the criminal conduct may occur in a specific country, the party launching the attack is not necessarily a sovereign state, and may even forge the source of the attack by various technical means, so that the attack is difficult to trace. This throws into relief, from another side, the fragility and complexity of international consensus on cybersecurity.

4 A New Concern: Data Security in the Course of Digitalisation

Confronted with the multiple predicaments of cybersecurity at home and abroad, India has become increasingly aware of the importance of cyber sovereignty to national development. The pluralist path presented by India's cybersecurity strategy is grounded precisely in this basic understanding of cyber sovereignty. The issue of data security is the core cornerstone of cybersecurity governance and determines the rationality, completeness and sustainability of cybersecurity strategy. The labelling of "data nationalism" precisely reflects India's heightened attention to data security in international cooperation; at the same time, this position has not prevented India from actively participating in international collaboration under the

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

conception of pluralism. On this basis, India is accelerating the construction of an integrated artificial intelligence and data platform.

4.1 Data Nationalism

The political expression of "data localisation" is "data nationalism", which is presented in actual data security governance through pluralist discursive means. Resolutely advancing data localisation is not only a clear declaration by India of its cyber sovereignty but also represents its choice of self-protection under actual conditions. Against the background of the rapid rise in the offensive and defensive cyber capabilities of such major countries and regions as the United States, China, Russia and the European Union, India's promotion of data localisation, and its adoption of a path of "inward orientation" in order to counter powerful external forces, have become an important strategy of self-defence.

At present India has grown into the world's third largest country in terms of internet users, after the United States and China, with an average annual growth rate exceeding 30 per cent, and it faces the severe challenge of how to protect users' privacy and information security. Since Modi took office, the increasingly pronounced nationalist colouring of the Indian government has won wide acceptance among India's internet users and has extended further from physical space into cyberspace. Modi's successive election victories are inseparable from his skilful use of online media and social media. For the Indian government, the guidance of online public opinion and of social media bears not only on the direction of public opinion but may also become a "catalyst" for nationalist sentiment. The Mumbai terrorist attacks, for example, produced a major tragedy; Lashkar-e-Taiba (LeT), a Pakistani armed jihadi organisation, began at the start of this century to recruit telecommunications engineers, technicians and operations personnel, and even designed its own applications and developed software, recruiting among young Muslims. Cybersecurity incidents have forced India to issue and refine the *Information Technology Act* and other relevant legislation.

On 1 March 2024 India's Ministry of Electronics and Information Technology (MeitY) published an *AI Advisory*, requiring all online platforms operating in India to provide the Indian government with operational reports. These reports cover data platforms with vast numbers of users, including Facebook, Instagram, YouTube, Twitter, Microsoft and LinkedIn. "Data nationalism" constitutes the distinctive undertone of India's data security protection and is driving its pluralist path of cybersecurity strategy gradually towards maturity.

4.2 Data Security in International Cooperation

The United States is India's most important partner in the field of cybersecurity, and one of the core challenges the two countries face in their cooperation is data security. As early as 2006 the United States and India launched a "cyber security forum", devoted to resolving issues of national security arising from the outsourcing of critical network information systems, knowledge management, software development and data processing, and from the growing interdependence of the two countries, with the aim of strengthening interaction between the two governments[15]. At that time India laid emphasis on research and development for capacity-building, while the United States was chiefly concerned with data protection. Because India's development in information technology innovation has been relatively slow, India's critical network information infrastructure (including the banking system, high-technology companies and the electricity grid) remains antiquated, while the digitalisation of India's critical infrastructure has fallen far short of a comparable level, making it difficult to meet the needs of the digital age. Nevertheless, the two countries still urgently need to explore and cooperate in the field of cybersecurity, for the reason not only that India has taken on a large volume of low-end internet business from the United States but that other multiple factors are involved as well—for example, the world's two largest submarine cable operators (Reliance Communications and Tata Communications) are both Indian enterprises and carry a large share of global internet traffic, and many Indian websites are also hosted on servers in the United States.

In order to restrain cybercrime effectively, both the United States and India recognise the importance of real-time response and information sharing. However, the channels of cooperation currently available to the two countries still depend mainly on Interpol and on mutual legal assistance treaties. In the field of counter-terrorism, because the United States' strategy in Central and South Asia converges with India's position in Central Asia, the two countries have a relatively strong willingness to cooperate and a relatively broad consensus in combating terrorism. Beyond this, joint research and development ought to have become another potential field of cooperation, but it needs to be founded on an open academic environment and on platforms for scientific research. Intercepting and breaking encrypted communications is one of the important means of cybersecurity, and where the US government imposes export controls on encryption technology, obstacles remain considerable for the two sides in sharing technology. At present the two countries hold markedly different positions on data: the United States advocates data sharing in order to ensure its unimpeded passage through the cyber world, while India resolutely opposes large-scale data sharing, pursues "data nationalism" and treats data protection as a priority—which is inseparable from the relative weakness of India's capacity for cybersecurity protection and from its practical need to pursue self-defence.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

India once enjoyed a certain reputation in the field of healthcare. However, because India still lacks capacity in data protection, how to protect health information has become a major problem. In addition, the spread of electronic money has provided the Indian people with more diversified means of payment, and the personal financial risk has risen markedly with it.

4.3 Building an Integrated Artificial Intelligence and Data Platform

In the age of intelligent technology, the issue of data security has become a core concern of the Indian government. As early as 2018 the Indian government had already turned its attention to the potential risks that artificial intelligence might bring and had begun to formulate corresponding responses. On 1 February of that year, the then Finance Minister Arun Jaitley observed in his annual budget report that the global economy is being transformed into a digital economy by the application of cutting-edge technology in digital space, including such frontier technologies as machine learning, artificial intelligence, the Internet of Things and 3D printing. To this end the National Institution for Transforming India (NITI Aayog) would launch a national programme to guide research and application in the field of artificial intelligence in India. In January 2020 that think tank published a further approach paper, *Artificial Intelligence Cloud Computing Specific Infrastructure Construction*, setting out the goal of building an integrated platform for artificial intelligence research, analysis and data (AIRAWAT).

The advancement of "Digital India" has carried Indian society smoothly through the transition from the era of the informatisation outsourcing industry to the internet era and further towards comprehensive digitalisation. Data analysis, however, imposes a higher demand for computing power on hardware infrastructure, and many of India's internet applications still rely on high-performance servers in the United States for support. The integrated platform for artificial intelligence research, analysis and data has therefore become the key link through which India may "catch up" in the new round of the global technological wave, and whether it can genuinely make up the shortfall in technological iteration is particularly important. To address the high cost and low availability that continue to afflict the development, training and deployment of computing infrastructure, NITI Aayog submitted to the government, on the basis of the *National Strategy for Artificial Intelligence*, a series of approach papers including *AIRAWAT: An AI Cloud Computing Infrastructure for India*. The paper recommends building an underlying foundational cloud service to promote the development of artificial intelligence research and solutions in India, employing high-performance, high-throughput supercomputing technology. The system is intended to improve efficiency in such fields as healthcare, education, agriculture and transport, while providing strong support in three respects—computing capacity, data storage and the scale of digital data—bringing an entirely new solution to the Indian government and to its network governance needs. The framework of the integrated platform is shown in Figure 1.

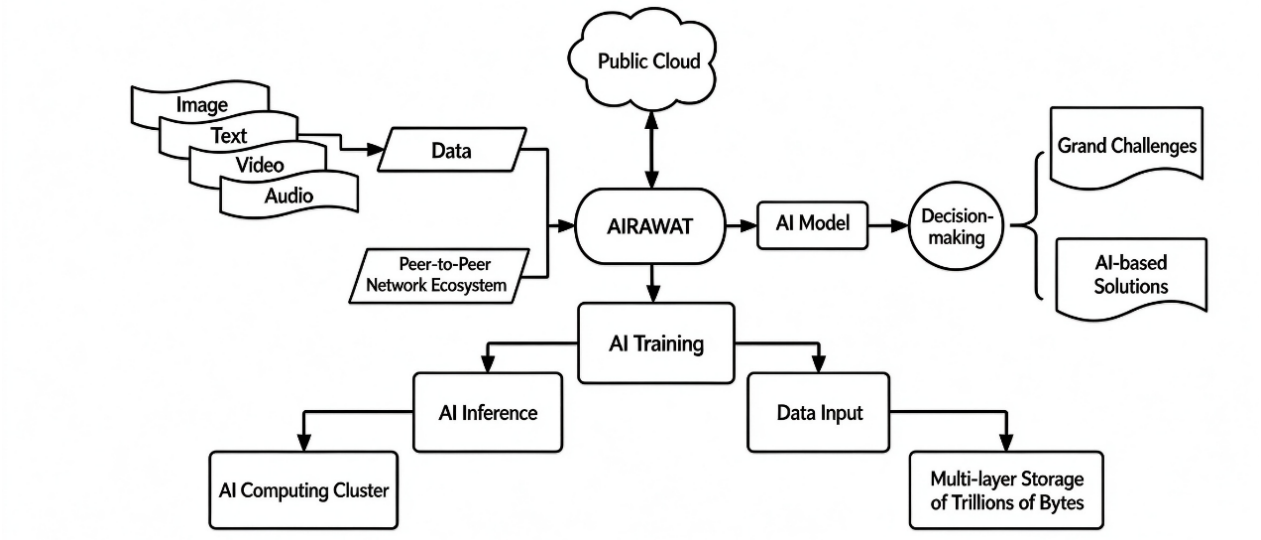


Figure 1 Framework of the integrated platform

The AIRAWAT platform is planned to build high-performance data storage space and leading data processing capacity, achieving data autonomy and more complete data analysis functions. At present the AIRAWAT platform is still at the design stage: the implementing party, the source of funding, the regulatory body and the provision of intellectual support have yet to be settled, and the scale the platform may ultimately attain also remains uncertain. From a technological

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

standpoint, India's network governance is gradually shifting from legislative guidance towards a greater emphasis on data autonomy and data security. The shift in the centre of gravity of management means that governance capacity changes with it. Although the supporting means and the governance model of India's data security still need time to be put into practice and tested, the proposal of the AIRAWAT platform is undoubtedly of milestone significance, providing a substantive scheme for the concrete implementation of India's network governance.

5 Conclusion

The wave of information technology in the last century drove the modernisation of the Indian state and the rapid growth of its economy. "Digital India" is not only Modi's personal governing slogan but also India's strategic ambition. Looking back at the trauma of history and at choices in international strategy, one may perceive that India has displayed a distinctive national wisdom. Yet the mismatch between the state's will and its technological capacity brings marked challenges to domestic governance, and at the international level India likewise faces the structural tension induced by multiple predicaments. India's design of strategy and method for cybersecurity governance has always taken its own capacity as the benchmark. Even though India's wish to rank among the world's cyber powers is strong, it is inevitably limited by many internal and external factors—unbalanced cooperative relationships, the absence of international governance rules, the intricacy of regional politics and the inadequacy of its own core cybersecurity capacity—so that it can only adjust continually and pursue a pluralist path.

In the continuing evolution of its national cybersecurity strategy, India was among the first to recognise the key position of data security in the course of national digitalisation and has been particularly active in the contest over rule-formulation with the International Telecommunication Union and the Western countries. The shift in India's diplomatic strategy from "non-alignment" to "multi-alignment" [10] is likewise reflected in the changes in its cybersecurity strategy. India's choice in cybersecurity strategy does not attach itself to any particular alliance, which is closely bound up with its actual capacity and also expresses its distinctive conception. In its cybersecurity strategy the Indian government has chosen pluralism rather than a simple hedging approach. At the same time, India is actively issuing a national strategy for artificial intelligence and formulating concrete pathways, laying a foundation for the next stage of development; the changes this brings in the defence field win it an early advantage in responding to possible external conflicts and further consolidate its leading position in South Asia.

References

[1] Luo X. Research on the development of India's cyberspace security industry[J]. Information Security and Communications Privacy, 2023(12): 27-34. [in Chinese]

[2] He H, Yang QQ. The current state of and difficulties in India's legislation against online violence[J]. Modern World Police, 2023(7): 60-65. [in Chinese]

[3] Bi SH, Lin YH, Geng X. The process, logic and challenges of Japan-India digital cooperation under the Indo-Pacific framework[J]. Indian Ocean Economic and Political Review, 2023(6): 81-98. [in Chinese]

[4] Zhang SJ. US-India cybersecurity competition and cooperation from the perspective of India's cybersecurity governance[J]. Information Security and Communications Privacy, 2019(8): 63-74. [in Chinese]

[5] Wang YC, Song DX. US-India cybersecurity cooperation: external transformation, endogenous drivers and the proliferation of contradictions[J]. South Asian Studies, 2023(1): 70-96. [in Chinese]

[6] Zhang ZQ. An overview of India's capacity-building in cyberspace[J]. China Information Security, 2022(9): 79-83. [in Chinese]

[7] Rong GJ. An analysis of the process of India's participation in the international governance of cyberspace[D]. Beijing: China Foreign Affairs University, 2020. [in Chinese]

[8] Dai YH, Chen SQ. India's data localisation: collisions and opportunities in the frontier of cyber interests[J]. South Asian Studies Quarterly, 2022(2): 93-112. [in Chinese]

[9] Hua JF. The construction of India's cybersecurity system[J]. Information Security and Communications Privacy, 2022(6): 21-31. [in Chinese]

[10] Li L. From non-alignment to "multi-alignment": a study of the hedging character of India's foreign strategy[J]. World Economics and Politics, 2020(12): 21. [in Chinese]

[11] Das C P. Make in India: an analysis of IT sector[J]. Splint International Journal of Professionals, 2017: 69.

[12] Kapur Devesh. The causes and consequences of India's IT boom[J]. India Review, 2002, 1(2): 91-110.

[13] Nehru J. *Glimpses of World History*[M]. Gao Y, trans. Beijing: Peking University Press, 2016. [in Chinese]

[14] Mao WZ, Liu YS. Data nationalism: driving logic and policy influence[J]. Global Review, 2020, 12(3): 20-42. [in Chinese]

[15] Samuel C. Prospects for India-US cyber security cooperation[J]. Strategic Analysis, 2011, 35(5): 770-780.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.