



RECONCEPTUALISING STATE CAPACITY IN THE DIGITAL ERA: INSTITUTIONAL TRANSFORMATION AND PUBLIC SERVICE DELIVERY IN INDIA

Dr. Punamdeep Singh

Assistant Professor & Head, Department of Public Administration, G.S.S.D.G.S Khalsa College, Patiala

ABSTRACT

Digitalisation is transforming the institutional foundations of contemporary governance. Traditionally, state capacity has been understood in terms of administrative organisation, fiscal resources, legal authority, human resources and the ability of governments to implement public policies. In the digital era, these conventional dimensions are increasingly supplemented by digital infrastructure, data governance, interoperability, cybersecurity, digital competencies and algorithmic accountability. Digital transformation therefore represents not simply the adoption of new technologies but a broader restructuring of administrative institutions and public-service delivery.

India provides an important context for examining this transformation. Initiatives such as Digital India, Aadhaar, Unified Payments Interface (UPI), DigiLocker and other components of digital public infrastructure have created an increasingly interconnected digital ecosystem. These developments have expanded opportunities for integrated service delivery, information sharing, administrative coordination and citizen access. At the same time, they have generated new institutional challenges relating to privacy, cybersecurity, digital exclusion, fragmented administrative capacity and the governance of artificial intelligence.

This paper conceptually examines the transformation of state capacity in the digital era, with particular reference to India. It is based on secondary sources, including scholarly literature, government reports, policy documents, legislation and institutional publications. The paper argues that digitalisation does not replace traditional state capacity; rather, it extends and restructures it. It proposes a multidimensional Digital State Capacity Framework consisting of digital infrastructure, interoperability, human capacity, data capacity, accountability, security and privacy, inclusion and service capacity. The paper concludes that the effectiveness of digital governance should be assessed not merely through the number of digital services but through the capacity of institutions to convert technological resources into accessible, accountable, secure and citizen-centred public value.

KEYWORDS: State Capacity, Digital Governance, Digital Transformation, Digital Public Infrastructure, Public Service Delivery, Institutional Transformation, India

1. INTRODUCTION

State capacity is a central component of effective governance and refers broadly to the ability of governments to formulate and implement policies, mobilise resources, regulate social and economic activities and provide public services. Traditionally, it has been associated with the strength of administrative institutions, fiscal resources, legal authority, organisational coordination and human capabilities.¹ Nevertheless, the formal existence of institutions alone does not guarantee effective governance. Their actual capacity is reflected in their ability to implement governmental decisions and convert them into meaningful administrative and societal outcomes.²

State capacity encompasses the ability of public institutions to exercise authority and implement decisions

within society. In this context, infrastructural capacity refers to the state's reach into society and its ability to effectively enforce decisions within its jurisdiction. Furthermore, the development of effective state institutions relies on sustained investment in legal and fiscal capabilities, enabling governments to enforce regulations, mobilise resources and perform essential public functions.³ Thus, state capacity ultimately concerns not only the possession of formal authority but also the institutional ability to coordinate resources, implement decisions and achieve intended outcomes.

The rapid expansion of digital technologies has significantly altered the environment in which state capacity operates. Government institutions increasingly depend upon digital platforms, databases, cloud-based systems, interoperable technologies, digital identities, data analytics and automated decision-support mechanisms. As a result, administrative effectiveness is becoming increasingly

¹ Galileu Kim, Tanu Kumar, Rita Ramalho, and Stuart Ehrlich Russell, *Institutional Capacity for Policy Implementation: An Analytical Framework*, World Bank Policy Research Working Paper 11279 (Washington, DC: World Bank, 2026), pp. 4–7.

² Michael Mann, "The Autonomous Power of the State: Its Origins, Mechanisms and Results," *European Journal of Sociology* 25, no. 2 (1984): 185–213, especially p. 189.

³ Timothy Besley and Torsten Persson, "The Origins of State Capacity: Property Rights, Taxation, and Politics," *American Economic Review* 99, no. 4 (2009): p. 1219.



dependent on technological infrastructure and the capacity to generate, manage, exchange and utilise information.⁴

Therefore, digital transformation should be understood as more than the conversion of conventional administrative procedures into electronic formats. It has the potential to reshape organisational structures, administrative processes and the relationship between government institutions and citizens. Key characteristics of digital-age governance include enhanced organisational integration, a more comprehensive approach to addressing citizens' needs and the increasing use of digital technologies in administrative processes. Similarly, the evolution of digital government signifies a progression from basic digitisation towards broader institutional transformation, citizen engagement and context-specific digital governance.⁵

India offers a significant context for examining this transformation. Initiatives such as Digital India, Aadhaar, the Unified Payments Interface (UPI), DigiLocker and other components of digital public infrastructure have contributed to the development of an increasingly interconnected administrative ecosystem. Digital technologies are now being used not only for providing online service delivery but also for authentication, digital payments, information exchange, record management and coordination among public institutions.⁶

The rapid expansion of digital public services is reflected in the National e-Governance Service Delivery Assessment (NeSDA). According to the January 2026 assessment, 24,563 e-services were available across States and Union Territories, while more than 81 per cent of mandatory e-services had achieved saturation (fully available). Local governance and utility services constitute the largest category; comprising 8,846 services.⁷ These developments indicate the growing institutionalisation of digital service delivery within India's administrative system.

However, the expansion of digital infrastructure and online services does not, by itself, guarantee robust state capacity. Effective digital governance requires capable institutions, adequately trained personnel, reliable technological infrastructure, high-quality data, system interoperability and appropriate accountability mechanisms.

⁴ OECD, *Digital Government Outlook 2026: From Foundations to Transformational Impact* (Paris: OECD Publishing, 2026), p. 15.

⁵ Tomasz Janowski, "Digital Government Evolution: From Transformation to Contextualization," *Government Information Quarterly* 32, no. 3 (2015): pp. 221–223.

⁶ OECD, *Digital Public Infrastructure for Digital Governments, OECD Public Governance Policy Papers*, no. 68 (Paris: OECD Publishing, 2024), pp. 4–8.

⁷ Department of Administrative Reforms and Public Grievances, Government of India, *NeSDA—Way Forward Monthly Report for States/UTs, January 2026* (New Delhi: Government of India, released February 17, 2026), https://darpg.gov.in/sites/default/files/NeSDA_WF_Jan26_Report_V9.pdf. See also Press Information Bureau, Government of India, "33rd Edition of the NeSDA—Way Forward Monthly Report for States/UTs Released," February 17, 2026, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2229287&lang=1®=3>.

At the same time, increasing dependence on digital systems raises concerns relating to privacy, cybersecurity, unequal access, data protection and the accountability of automated decision-making.⁸

The central argument of this paper is that digitalisation does not replace the traditional foundations of state capacity; rather, it expands, modifies and restructures them. The digitally capable state therefore requires a combination of conventional administrative, legal and organisational strengths with new technological, informational and institutional capabilities. Understanding this transformation is essential for assessing the changing nature of public administration and public-service delivery in India.

2. CONCEPTUALISING STATE CAPACITY

State capacity broadly denotes the ability of public institutions to formulate and implement policies, mobilise resources, regulate social and economic behaviour and provide public goods and services. It encompasses both the institutional arrangements through which governmental authority is exercised and the organisational, financial and human resources required to translate decisions into effective action. Thus, state capacity is not determined merely by the formal existence of institutions; it is also reflected in their practical ability to implement public decisions and achieve intended outcomes.⁹

An important dimension of state capacity is the ability of the state to reach across society and implement decisions throughout its territorial jurisdiction. This dimension, commonly described as infrastructural power, emphasises the practical reach and implementation capacity of state institutions rather than the mere possession of formal authority.¹⁰ A government may possess extensive legal powers, but if its administrative institutions lack the necessary organisational reach or logistical mechanisms necessary to implement those decisions, its effective capacity remains limited.

Furthermore, state capacity also possesses important legal and fiscal dimensions. Legal capacity enables public institutions to establish and enforce rules, protect rights and support well-functioning markets, while fiscal capacity empowers governments to mobilise revenues and finance public functions. These dimensions are deeply interconnected, as sustained institutional investment in legal and fiscal capacity strengthens a government's ability to regulate economic activity, enforce contracts and mobilise resources.¹¹

Administrative capacity constitutes another essential component of state capacity. Effective implementation depends upon appropriate organisational structures, competent personnel, coordination mechanisms, institutional continuity

⁸ OECD, *Digital Government Outlook 2023* (Paris: OECD Publishing, 2023), pp. 31–37.

⁹ Francis Fukuyama, "What Is Governance?" *Governance* 26, no. 3 (2013): pp. 350–352.

¹⁰ Mann, "The Autonomous Power of the State," p. 189.

¹¹ Besley and Persson, "The Origins of State Capacity," pp. 1219–1220.



and reliable administrative procedures.¹² Therefore, traditional state capacity can be understood as the combined ability of public institutions to exercise legitimate authority, mobilise resources, coordinate administrative activities and implement public decisions effectively.

However, the emergence of digital technologies does not displace these foundational dimensions of state capacity. Rather, it introduces additional technological and informational requirements into their operation. Contemporary governments increasingly rely on digital infrastructure, information systems, databases and digital platforms to perform administrative functions and deliver public services.¹³ This development suggests that the effectiveness of traditional administrative, legal, fiscal and human capabilities is increasingly influenced by the availability and effective management of technological and informational resources.

The essence of this discussion is that digital state capacity can be conceptualised as expanding and restructuring traditional state capacity by integrating technical, informational and digital capabilities into government institutions and processes. It encompasses public institutions' ability to align their administrative, legal, financial and human resources with digital infrastructure, data, interoperable systems and technical expertise to formulate and implement public decisions and deliver public services effectively, securely, responsively and inclusively.

3. DIGITAL TRANSFORMATION AND STATE CAPACITY

Digital transformation represents a shift in the way government institutions organise processes, coordinate activities and interact with citizens. It is therefore not limited to converting paper-based procedures into electronic formats. Rather, it involves the restructuring of administrative processes, the integration of government functions and the development of public services that are more accessible, coordinated and responsive.¹⁴ Its significance for state capacity lies in the possibility of altering how public institutions acquire information, coordinate decisions, allocate resources and implement policies.

One important mechanism through which digital transformation can affect state capacity is administrative integration. Government functions that were previously distributed across separate departments can increasingly be connected through shared digital platforms, interoperable databases and integrated service-delivery systems. Such

arrangements can reduce duplication, facilitate information exchange and simplify citizens' interactions with multiple government agencies. Digital integration can therefore encourage a shift from department-centred administration towards more coordinated and citizen-centred forms of governance.¹⁵

A second mechanism is the transformation of administrative processes. Digital technologies can automate routine tasks, accelerate the processing of information, improve record management and facilitate real-time access to administrative data. As digital systems become embedded within organisational processes, they can alter not only the speed of administrative operations but also the ways in which decisions are formulated, monitored and implemented. Janowski's evolutionary approach is useful here because it demonstrates how government use of digital technologies can progress from basic digitisation towards organisational transformation and context-specific forms of digital governance.¹⁶

A third mechanism concerns information and decision-making capacity. Digital systems can expand the state's ability to collect, integrate, analyse and use information for policy formulation and implementation. Data-driven administration can potentially improve monitoring, identify service-delivery gaps and support more evidence-based decision-making. However, these benefits depend upon the quality, accessibility and appropriate governance of data. Poor-quality information, fragmented databases or weak data-management practices can limit the contribution of digital technologies to administrative effectiveness.

Digital transformation also creates new institutional requirements. Interoperability, data governance, cybersecurity, digital skills, privacy protection and accountability become increasingly important as government functions become dependent upon interconnected technological systems.¹⁷ Thus, technological infrastructure by itself does not create stronger state capacity. Its contribution depends upon whether public institutions possess the organisational capabilities, human resources and governance arrangements required to use technology effectively and responsibly.

Finally, digital transformation can alter the relationship between the state and citizens. Online service delivery, digital identity systems, electronic payments and integrated service platforms can reduce transaction costs and improve accessibility. At the same time, unequal digital access, inadequate digital literacy, privacy risks and exclusion from technology-mediated services may create new forms of administrative inequality. Digital transformation can therefore strengthen state capacity only when technological innovation is accompanied by institutional responsiveness, accountability and inclusive service delivery.

The relationship between digital transformation and state capacity is consequently neither automatic nor exclusively

¹² Merilee S. Grindle, *"The Good Government Imperative: Human Resources, Organizations, and Institutions,"* Getting Good Government: Capacity Building in the Public Sectors of Developing Countries (Cambridge, MA: Harvard Institute for International Development, 1997), pp. 3–8.

¹³ OECD, *The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government* (Paris: OECD Publishing, 2020), pp. 8–17.

¹⁴ Patrick Dunleavy, Helen Margetts, Simon Bastow, and Jane Tinkler, *"New Public Management is Dead – Long Live Digital-Era Governance,"* Journal of Public Administration Research and Theory 16, no. 3 (2006), pp. 467–470.

¹⁵ Ibid.

¹⁶ Tomasz Janowski, *"Digital Government Evolution: From Transformation to Contextualization,"* pp. 221–223.

¹⁷ OECD, *Digital Public Infrastructure for Digital Governments*, 4–8.



technological. Digitalisation can strengthen existing administrative capabilities while simultaneously creating new institutional demands. The digitally capable state is therefore not simply a government equipped with advanced technologies; it is one that can effectively integrate technology, information and digital infrastructure into its administrative, legal and organisational capacities to produce effective, accountable and citizen-centred outcomes.

4. FROM E-GOVERNANCE TO DIGITAL GOVERNANCE IN INDIA

India's digital governance trajectory has progressed from the computerisation of administrative functions and individual e-governance initiatives towards integrated digital platforms and shared public digital infrastructure. The Digital India programme provided a broad policy framework for expanding digital connectivity, improving electronic service delivery and promoting digital empowerment.¹⁸ Subsequently, digital identity, digital payment systems, digital document repositories and authentication mechanisms contributed to the development of interconnected digital capabilities across administrative and social sectors.¹⁹

The significance of this transformation lies not merely in the expansion of digital applications but in the creation of shared technological infrastructure capable of supporting multiple public functions. Digital identity, digital payments, authentication and secure information exchange can facilitate the delivery of welfare benefits, financial services, official documents and other public services. Such infrastructure can strengthen administrative coordination, reduce procedural duplication and improve the accessibility of government services.²⁰ However, these benefits depend on effective institutional coordination, appropriate safeguards and the ability of public agencies to use digital systems responsibly.

The modular character of India's digital public infrastructure allows different technological components to be combined and adapted for diverse administrative and developmental purposes.²¹ This approach creates opportunities for innovation in public service delivery and enables institutions to build new applications using existing digital

capabilities. Nevertheless, the effective utilisation of these systems requires adequate technical expertise, institutional preparedness, data protection and accountability mechanisms.

The expansion of electronic service delivery provides an indication of the growing institutional adoption of digital governance. According to the January 2026 *National e-Governance Service Delivery Assessment (NeSDA) Way Forward* report, released in February 2026, States and Union Territories provided 24,563 e-services, of which 8,846 related to Local Governance and Utility Services. The report also recorded the addition of 473 e-services since the previous assessment.²² These figures demonstrate the increasing reach of digital service delivery, although the number of services alone does not establish their quality or effectiveness.

5. DIGITAL PUBLIC INFRASTRUCTURE AND STATE CAPACITY

Digital public infrastructure has become an important foundation of India's digital transformation. DPI differs from individual digital applications because it provides shared technological foundations that can support multiple services and institutions.

Digital identity, payment systems and data-exchange mechanisms illustrate this approach. Their institutional significance derives from interoperability and reusability. A common digital infrastructure can allow different organisations to build services upon shared foundations rather than creating completely independent systems.

Research on India's Digital Stack indicates that combinations of digital services can generate public value when they are used together rather than in isolation.²³ From a state-capacity perspective, DPI can reduce transaction costs, improve coordination and support more integrated service delivery.

However, shared infrastructure also creates shared vulnerabilities. A weakness in cybersecurity, data protection or governance can have consequences across several services. DPI should therefore be treated as an institutional resource whose effectiveness depends upon governance arrangements as much as technology.

6. INSTITUTIONAL TRANSFORMATION

Digital transformation can alter the internal organisation of government. Conventional administration has often relied upon hierarchical structures, departmental boundaries and sequential information flows. Digital systems facilitate faster

¹⁸ Government of India, Press Information Bureau, "Digital India – A Programme to Transform India into Digital Empowered Society and Knowledge Economy," August 20, 2014, sections "Vision Areas" and "Approach and Methodology,"

<https://www.pib.gov.in/newsite/PrintRelease.aspx?lang=2®=48&relid=108927>.

¹⁹ Ministry of Electronics and Information Technology, Government of India, "Government of India Taking Measures to Enhance the Reach of Indian Digital Public Infrastructure," Press Information Bureau, July 26, 2024,

<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2037598>.

²⁰ Ministry of Electronics and Information Technology, Government of India, "Digital Infrastructure," Digital India, <https://www.digitalindia.gov.in/digital-infrastructure/>.

²¹ Ashish Desai and Aroon P. Manoharan, "Digital Transformation and Public Administration: The Impacts of India's Digital Public Infrastructure," *International Journal of Public Administration* 47, no. 9 (2024): pp. 575–576.

²² Department of Administrative Reforms and Public Grievances, Government of India, NeSDA – Way Forward Monthly Report for States/UTs, January 2026, released February 17, 2026, https://darpg.gov.in/sites/default/files/NeSDA_WF_Jan26_Report_V9.pdf; see also Press Information Bureau, Government of India, 33rd Edition of the NeSDA – Way Forward Monthly Report for States/UTs Released, February 17, 2026, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2229287>.

²³ Ashish Desai, Aroon P. Manoharan, Sai Shiva Jayanth, and Sharlo Zack, "Public Value Creation Through Combined Consumption of Multiple Public Services – Case of India Stack," *International Journal of Public Administration* 47, no. 9 (2024): pp. 600–611.



information exchange and can enable greater horizontal coordination.

Interoperability is especially significant. When government systems can exchange information through common standards and secure interfaces, duplication can be reduced and administrative processes can become more integrated.

Digital transformation also changes the role of public officials. Officials increasingly need to work with data, digital platforms and technology-enabled workflows while coordinating across organisational boundaries.

This transformation is consistent with the OECD Digital Government Policy Framework, which identifies six dimensions of mature digital government: digital by design, data-driven public sector, government as a platform, open by default, user-driven government and proactiveness.²⁴ These dimensions indicate that digital government involves changes in administrative organisation, data use and citizen interaction rather than simply technological substitution.

Therefore, Institutional transformation requires changes in structures, procedures, skills and organisational culture.

7. DIGITAL GOVERNANCE AND PUBLIC-SERVICE DELIVERY

Public-service delivery represents one of the most visible areas in which digital transformation affects citizens. Online applications, digital certificates, electronic payments, digital identity systems and integrated portals can reduce the need for repeated physical visits to government offices.

Digital systems can also improve administrative transparency. Application tracking, electronic notifications and digital records can make administrative processes more visible and facilitate monitoring.

However, placing an existing procedure online does not necessarily improve service delivery. A complicated paper-based process can become an equally complicated digital process if administrative procedures are not redesigned.

Citizen-centred design is therefore essential. Digital government should be organised around the needs and experiences of users rather than simply reproducing departmental structures online. The OECD framework's emphasis on user-driven and proactive government reinforces this principle.²⁵

Digital service delivery must also account for citizens who lack connectivity, devices or digital literacy. Assisted access and alternative channels remain important components of inclusive digital governance.

8. HUMAN CAPACITY AND MISSION KARMAYOGI

Technology cannot function effectively without capable personnel. Digital government requires officials who can use digital tools, interpret data, manage technology-enabled

workflows and understand cybersecurity and data-protection requirements.

Mission Karmayogi represents an important institutional response to this requirement. The Karmayogi Competency Model identifies digital fluency and data analytics among relevant competencies. Digital fluency includes the effective use of digital tools and platforms, while data analytics encompasses data management, analysis, visualisation and data-led decision-making.²⁶

Human capacity is therefore a central component of digital state capacity. Training should extend beyond basic computer literacy to include data interpretation, digital service design, cybersecurity, artificial intelligence and technology governance.

The human dimension is particularly important because technological systems require administrative judgement. Digital transformation should strengthen rather than eliminate the capacity of officials to exercise informed and accountable decision-making.

9. DATA AS A NEW ADMINISTRATIVE RESOURCE

Data has become an increasingly important resource of contemporary administration. Government departments generate and use information relating to citizens, programmes, transactions, infrastructure and service delivery.²⁷ Well-managed data can support evidence-based policymaking, monitoring, evaluation and targeted interventions. Integrated datasets can also improve the ability of institutions to identify problems, anticipate needs and coordinate administrative responses. However, data is useful only when it is accurate, accessible, appropriately managed and securely protected. Fragmented, incomplete or poor-quality data can weaken evidence-based decision-making and reduce the effectiveness of administrative interventions.²⁸ Therefore, the emergence of data-driven administration requires institutional arrangements governing data collection, storage, sharing, quality, security and accountability. Effective data governance provides the institutional and technical foundations necessary for the responsible use and reuse of data across government.²⁹

In this context, the Digital Personal Data Protection Act, 2023 provides a statutory framework for the processing of digital personal data, recognising both the individual's right to protect their personal data and the necessity for lawful

²⁴ OECD, *The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government*, pp. 6 & 8–10.

²⁵ OECD, *The OECD Digital Government Policy Framework*, pp. 28–35.

²⁶ *Capacity Building Commission, Government of India, Karmayogi Competency Model (New Delhi: Capacity Building Commission), sections "Digital Fluency" and "Data Analytics,"* https://cbc.gov.in/sites/default/files/2026-01/KCM-Output_RestructuredOct17.pdf.

²⁷ *Organisation for Economic Co-operation and Development (OECD), The Path to Becoming a Data-Driven Public Sector (Paris: OECD Publishing, 2019), pp. 11–14.*

²⁸ OECD, *The Path to Becoming a Data-Driven Public Sector*, pp. 47–52.

²⁹ OECD, *The Path to Becoming a Data-Driven Public Sector*, pp. 29–39.



processing.³⁰ Consequently, data capacity must be developed together with privacy safeguards, security measures and responsible governance. Therefore, the administrative value of data depends not merely on its availability, but also on the state's institutional capacity to manage, integrate, protect and utilize it responsibly.

10. ARTIFICIAL INTELLIGENCE AND EMERGING ADMINISTRATIVE CAPACITY

Artificial intelligence is likely to become increasingly important in public administration. AI can assist government institutions in data analysis, forecasting, pattern recognition, service personalisation and administrative decision-making. Its growing relevance also creates new requirements for institutional, technical and human capacity within the public sector. India's IndiaAI Mission, approved by the Union Cabinet in March 2024 with an approved financial outlay of ₹10,371.92 crore over five years, seeks to strengthen the country's AI ecosystem through initiatives relating to computing capacity, innovation, datasets, application development, future skills, start-up financing and safe & trusted AI.³¹ Therefore, the Mission represents not only an investment in technological infrastructure but also an effort to develop the institutional and human capabilities required for responsible AI adoption.

However, the use of AI in government necessitates a workforce capable of understanding algorithmic systems, assessing their limitations and monitoring their performance. Algorithmic accountability becomes particularly important where automated or AI-assisted systems influence public benefits, regulatory decisions or access to government services. In such contexts, administrative institutions must retain mechanisms for human oversight, review, explanation and correction. Consequently, the development of AI capabilities must be accompanied by appropriate governance frameworks to address issues such as bias, transparency, accountability, privacy and security. As a result, AI represents an opportunity to strengthen administrative capacity and a new area of governance responsibility.³²

11. PRIVACY, CYBERSECURITY AND DIGITAL ACCOUNTABILITY

The expansion of digital government has increased both the volume and importance of information held and processed by public institutions. Consequently, privacy and cybersecurity have become vital components of contemporary state capacity. Government information systems support essential public services, financial transactions and administrative processes; thus, security and continuity of these

³⁰ Government of India, The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, Preamble and Sections 4–8, pp. 1 & 7–11.

³¹ Government of India, Press Information Bureau, IndiaAI Mission, Government of India, 2025, pp. 1–2.

³² Government of India, Press Information Bureau, "Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem," 7 March 2024, pp. 1–2.

systems are crucial for effective governance.³³ Therefore, cybersecurity is not merely a technical concern but also an institutional and administrative responsibility, as disruption, unauthorised access or compromises within government systems can impact service delivery and public trust. So privacy is equally significant. While there is no doubt that the integration and processing of data can improve service delivery and administrative coordination, the extensive collection and processing of personal information can also create risks related to unauthorised access, misuse, and inappropriate disclosure.

The Digital Personal Data Protection Act, 2023 establishes a statutory framework for the processing of digital personal data while recognising the right of individuals to protect their personal data and the need to process such data for lawful purposes.³⁴ The Act further establishes provisions concerning notice, consent, legitimate uses, obligations of data fiduciaries, rights of data principals and grievance redressal. Digital accountability also requires mechanisms through which administrative actions can be traced, monitored and reviewed. Digital records, audit trails, grievance mechanisms and monitoring systems can strengthen accountability when supported by appropriate institutional arrangements. Therefore, the challenge is to develop digital systems that are simultaneously efficient, secure, transparent and rights-sensitive. Consequently, privacy, cybersecurity and accountability should be treated not as external constraints on digital state capacity but as essential aspects of a capable, responsible and trustworthy digital state.³⁵

12. DIGITAL DIVIDE AND INCLUSIVE GOVERNANCE

There is no doubt that digitalisation has significantly improved access to government services, but unequal access to digital technologies has also created new forms of exclusion. Disparities in internet connectivity, digital literacy, income, gender, age, disability and geographical location can affect citizens' ability to access and effectively use online government services. Therefore, digital divide is not merely a technological problem but also an institutional and social issue; because the mere availability of an online service does not necessarily ensure that all citizens can access it.³⁶

Inclusive digital governance requires focus on accessibility, user-oriented design, multilingual services, assisted digital access and alternative channels for citizens who are unable or unwilling to use digital platforms

³³ World Bank, GovTech Maturity Index, 2022 Update: Trends in Public Sector Digital Transformation (Washington, DC: World Bank, 2022), pp. 4–8.

³⁴ Government of India, The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 (New Delhi: Government of India, 2023), Preamble, p. 1.

³⁵ OECD, The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government, pp. 8–17.

³⁶ United Nations Department of Economic and Social Affairs (UNDESA), United Nations E-Government Survey 2022: The Future of Digital Government (New York: United Nations, 2022), pp. 31–34.



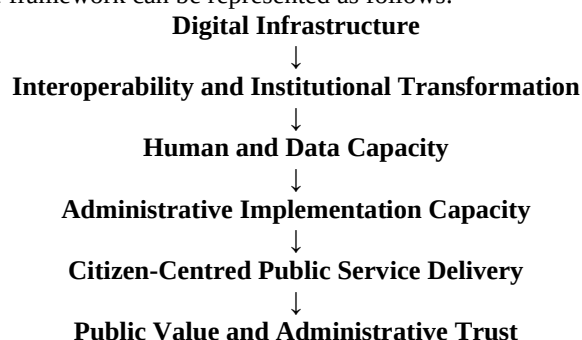
independently.³⁷ This is particularly important at the local level, where citizens may require assistance in completing applications, uploading documents, authenticating information or navigating government portals. Therefore, the objective of digitalisation should be to reduce administrative burdens, rather than simply transfer those burdens from government offices to citizens. Consequently, the goal of digital transformation should not merely be to increase the number of services available online; instead, it should also ensure that citizens—regardless of their varying levels of technical access and capability—can have effective and equal access to these services.³⁸

13. PROPOSED DIGITAL STATE CAPACITY FRAMEWORK

The preceding analysis suggests that ‘digital state capacity’ should be understood as a multidimensional institutional capability rather than as the simple possession of digital technologies. It encompasses the technological, organisational, human, informational, regulatory and citizen-oriented capabilities required to use digital systems effectively for public purposes. Accordingly, the framework proposed here combines digital infrastructure with interoperability, human and data capacity, accountability, security, inclusion and service-delivery capacity.³⁹

DIMENSION	MAJOR COMPONENTS
Digital Infrastructure	Connectivity, platforms, cloud systems and digital identity
Interoperability	APIs, common standards and secure information exchange
Human Capacity	Digital fluency, data analytics and AI-related skills
Data Capacity	Data quality, management, integration and analysis
Accountability	Audit trails, monitoring, transparency and grievance redress
Security and Privacy	Cybersecurity, data protection and risk management
Inclusion	Accessibility, assisted access and alternative channels
Service Capacity	Integrated, user-centred and end-to-end digital services

The framework can be represented as follows:



This framework highlights that technology constitutes only one component of digital state capacity. Digital infrastructure must be integrated with institutional coordination, competent personnel, effective data governance, accountability, security and social inclusion. Interoperability is particularly important because fragmented digital systems can reproduce the departmental silos of conventional administration, whereas common standards and integrated platforms can facilitate information exchange and delivery of coordinated services.⁴⁰ Similarly, human capacity remains essential because digital systems require officials who possess technological, analytical and managerial competencies. Data governance and cybersecurity provide additional institutional foundations for ensuring that digital resources are reliable, secure and used responsibly.

Therefore, the framework conceptualises digital state capacity as a transformation of existing administrative capabilities, rather than a separate technological capacity. The ultimate objective is not technological sophistication in itself, but the development of institutional capabilities that enable public organisations to implement policies effectively and provide accessible, responsive and trustworthy services.

14. TRADITIONAL AND DIGITAL STATE CAPACITY: A COMPARISON

Digital state capacity should not be viewed as a replacement for traditional state capacity. Rather, digital capabilities extend and modify existing administrative capacities. The transformation involves changes in the technological environment through which established administrative functions are performed, while core requirements such as institutional authority, organisational coordination, human judgement and accountability remain important.⁴¹ A comparative overview of some aspects of this transformation is presented here:

³⁷ OECD, *Digital Government Review of Sweden: Towards a Data-Driven Public Sector* (Paris: OECD Publishing, 2019), pp. 53–55.

³⁸ United Nations Department of Economic and Social Affairs, *United Nations E-Government Survey 2022*, pp. 34–39.

³⁹ World Bank, *GovTech Maturity Index, 2022 Update: Trends in Public Sector Digital Transformation* (Washington, DC: World Bank, 2022), pp. 4–8.

⁴⁰ OECD, *Digital Public Infrastructure for Digital Governments*, pp. 4–8; Government of India, *The Digital Personal Data Protection Act, 2023*, Act No. 22 of 2023, Preamble and Sections 4–8, pp. 1 & 7–11.

⁴¹ Tomasz Janowski, “Digital Government Evolution: From Transformation to Contextualization,” pp. 221–223.



TRADITIONAL STATE CAPACITY	DIGITAL STATE CAPACITY
Administrative hierarchy	Networked and interoperable institutions
Physical infrastructure	Digital infrastructure and platforms
Paper-based information	Data-driven administration
Departmental coordination	Real-time digital coordination
General administrative skills	Digital, analytical and technological skills
Conventional accountability	Digital audit trails and monitoring
Physical service delivery	Integrated online and assisted delivery
Conventional regulation	Technology and data governance
Administrative records	Interoperable digital information systems

The above comparison demonstrates that digitalisation expands the range of capabilities required by contemporary states. Conventional administrative authority, organisational structures and human judgement remain essential, but they increasingly operate through digital systems. Consequently, administrative capacity is being reconfigured rather than displaced. Hierarchical structures increasingly interact with networked platforms; paper-based records are supplemented or replaced by interoperable information systems; and conventional administrative skills are complemented by digital, analytical and technological competencies.⁴²

Furthermore, digital capacity introduces requirements that were less prominent in traditional administrative systems, including interoperability, data governance, cybersecurity, algorithmic accountability and digital inclusion. Consequently, a digitally capable state must possess both the foundational capacities associated with conventional administration and the additional institutional capabilities required to operate effectively in a digital environment.

Thus, the comparison supports the central proposition of this study: digital state capacity is an extension and reconfiguration of traditional state capacity. Digitalisation transforms the tools through which the state gathers information, coordinates institutions, implements policies and delivers services, however it does not eliminate the fundamental importance of administrative authority, institutional organisation, human judgement and public accountability.

15. MAJOR FINDINGS

- Expansion of State Capacity:** Digital transformation has expanded the meaning of state capacity by adding technological, informational and digital capabilities to conventional institutional and administrative resources.
- Role of Digital Public Infrastructure:** Digital public infrastructure has strengthened administrative coordination by enabling interoperable systems,

reducing duplication and supporting integrated public-service delivery.

- Importance of Human Capacity:** Technology cannot replace competent public officials. Digital transformation requires personnel with digital, analytical and technological skills alongside conventional administrative judgement.
- Data as an Administrative Resource:** Data has become a strategic resource for policymaking, monitoring and service delivery. Its effectiveness depends upon quality, interoperability, appropriate management and protection.
- Improvement in Public-Service Delivery:** Digital governance can simplify procedures, reduce transaction costs, improve accessibility and enhance transparency, provided that digital services are designed around citizens' needs.
- Emerging Accountability Challenges:** Digitalisation creates new accountability concerns relating to privacy, cybersecurity, data protection and automated decision-making, requiring stronger oversight and grievance mechanisms.
- Importance of Digital Inclusion:** Digital governance can create new forms of exclusion because of differences in digital literacy, connectivity, income, age, disability and geographical location.
- Reduction of Administrative Burdens:** Effective digitalisation should simplify administrative procedures rather than transfer the burden of navigating complex processes from government officials to citizens.
- Multidimensional Nature of Digital State Capacity:** Digital state capacity comprises infrastructure, interoperability, human and data capacity, security, accountability, inclusion and service-delivery capabilities rather than technology alone.
- Reconfiguration of Traditional Capacity:** Digital state capacity does not replace traditional state capacity; rather, it extends and reconfigures existing administrative institutions, skills and processes through digital systems.

16. MAJOR CHALLENGES

- Institutional Fragmentation:** Different government departments and administrative levels operate under separate digital systems and databases. Lack of interoperability between these systems restricts information sharing and coordination. This can weaken integrated governance and lead to a duplication of administrative efforts.
- Uneven Administrative Capacity:** Government institutions differ considerably in terms of infrastructure, financial resources, human resources and technological capabilities. Such variations affect their ability to adopt and manage digital systems effectively. Consequently, digital-governance

⁴² OECD, *The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government*, p. 8.



outcomes remain uneven across institutions and regions.

- iii. **Skill Gaps:** Due to rapid technological changes, there is a persistent shortage of competencies related to digital, analytical, cybersecurity, and artificial intelligence (AI) domains among government officials. This existing gap in skills limits the effective utilisation of new technologies. Therefore, continuous professional development is essential to maintain digital administrative capacity.
- iv. **Digital Exclusion:** Citizens who lack adequate internet access, appropriate devices, or digital literacy face difficulties in accessing online services. These barriers disproportionately affect vulnerable and marginalised groups. Consequently, if mechanisms are not established to ensure equal access for all, digitalisation could further exacerbate existing inequalities.
- v. **Privacy and Cybersecurity:** Greater dependence on digital systems increases exposure to cyberattacks, data breaches and unauthorised access. Weak security disrupts essential services and undermines public confidence. Therefore, privacy protection and cybersecurity must be integral components of digital governance.
- vi. **Algorithmic Accountability:** The increasing use of artificial intelligence raises concerns regarding transparency, explainability, human oversight and responsibility for errors. Automated systems may influence administrative decisions without being easily understood by citizens. Therefore, appropriate mechanisms for review, accountability and human intervention are essential.
- vii. **Measurement Limitations:** The number of online services provides only a partial measure of digital state capacity. A larger number of digital services does not necessarily indicate better administrative performance. Therefore, greater attention should be given to service quality, institutional effectiveness, citizen experience and outcomes.

17. SUGGESTIONS

- i. **Develop Digital State Capacity Indicators:** Government institutions should develop systematic indicators for assessing digital state capacity. These should cover infrastructure, interoperability, human resources, data governance, cybersecurity, inclusion and service outcomes. Such indicators can support benchmarking and institutional improvement.
- ii. **Strengthen Digital Competencies:** Continuous training of public officials should include digital literacy, data analytics, cybersecurity, AI governance and digital-service design. Training programmes should be regularly updated according to technological developments. This can strengthen both individual skills and organisational capacity.
- iii. **Improve Interoperability:** Common technical standards, secure APIs and institutional mechanisms for sharing information across government

departments should be strengthened. Improved interoperability can reduce administrative fragmentation and duplication. It can also facilitate coordinated and integrated delivery of public services.

- iv. **Adopt Citizen-Centred Service Design:** Government services should be redesigned around citizens' needs, experiences and accessibility requirements. Administrative procedures should be simplified before being digitised. This can prevent technology from merely reproducing complex procedures in digital form.
- v. **Maintain Assisted Digital Access:** Citizens facing technological, literacy or accessibility barriers should have access to assisted service channels. Digitalisation must provide alternative mechanisms for those unable to use online systems independently. This would help ensure that technological transformation remains inclusive.
- vi. **Strengthen Privacy and Cybersecurity:** Privacy protection and cybersecurity must be incorporated into the design of digital public infrastructure from the very beginning. They should not be treated merely as separate technical concerns. Robust security measures are essential for protecting citizens' information and maintaining institutional trust.
- vii. **Establish Responsible AI Governance:** As artificial intelligence becomes increasingly integrated into public administration, mechanisms for human oversight, transparency and accountability must be institutionalised. Administrative decisions influenced by AI should be subject to review and correction. Clear responsibility should also be established for errors and adverse outcomes.
- viii. **Shift Towards Outcome-Based Evaluation:** The assessment of digital governance should not be based solely on the number of services delivered online. Greater emphasis should be placed on accessibility, quality, accountability, citizen experience, and public value. Such an approach will provide a more meaningful evaluation of digital state capacity.

18. CONCLUSION

Digitalisation is transforming the institutional foundations of contemporary governance and expanding the meaning of state capacity beyond conventional administrative structures, fiscal resources, legal authority and human resources. Digital infrastructure, interoperability, data governance, technological competence, cybersecurity, privacy and algorithmic accountability have become increasingly important dimensions of administrative effectiveness.

India's experience illustrates the growing significance of this transformation. Initiatives such as Digital India, Aadhaar, UPI and DigiLocker have contributed to the development of interconnected digital public infrastructure and expanded the scope of electronic public-service delivery. The increasing availability of online services reflects the growing integration of digital technologies into administrative processes. However, technological advancement alone cannot guarantee



effective governance, as outcomes continue to depend upon institutional coordination, administrative competence and the ability to respond to citizens' needs.

Digitalisation should therefore be viewed as a means of strengthening, rather than replacing, conventional state capacity. Effective digital governance requires capable institutions, skilled public officials, appropriate legal frameworks and mechanisms to ensure transparency, accountability and the protection of citizens' rights. It must also address challenges relating to privacy, cybersecurity, institutional fragmentation and unequal access to digital services. Ultimately, reconceptualising state capacity in the digital era requires an integrated approach that combines technological innovation with institutional effectiveness, human competence and social inclusion. The success of digital governance in India will depend not merely on expanding digital infrastructure but on the ability of public institutions to use technology responsibly and deliver accessible, efficient, responsive and accountable public services.