

2026

Report on **Data Resilience** in India: A Framework for National Digital Security



© Copyright 2026 | Centre for Knowledge Sovereignty

All rights reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission from Centre for Knowledge Sovereignty.

This document contains information for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment.

This material is based on information that we believe to be reliable and adequately comprehensive, but we do not represent that such information is in all respects accurate or complete. Centre for Knowledge Sovereignty does not accept any liability for any losses resulting from use of the contents of this document.

Centre for Knowledge Sovereignty

A-99, Sector 47, Noida, Uttar Pradesh 201301

www.cksindia.in

ROUNDTABLES under the aegis of **VIKSIT BHARAT**

Strengthening data protection for a resilient economy

The Future Of Data Protection And Policy Making In India Balancing Innovation Regulation And National Security

📍 India habitat centre, New Delhi 📅 Monday 19 May 2025

Decoding the data dilemma sovereignty, strategy & security in the ai age

Building data resilience at scale : balancing innovation, regulation & national security in bharat's digital decade

📍 India habitat centre, New Delhi 📅 Tuesday 12 August 2025

Cyber resilience & data protection, a national imperative for critical infrastructure

Securing data, protecting future, empowering a resilient viksit bharat

📍 India habitat centre, New Delhi 📅 Tuesday 14 Oct 2025



Chief Guest Roundtable : 01



VIKSIT BHARAT : STRENGTHENING DATA PROTECTION FOR A RESILIENT ECONOMY

Theme

THE FUTURE OF DATA PROTECTION AND POLICY MAKING IN INDIA, BALANCING INNOVATION REGULATION AND NATIONAL SECURITY

 **19th May 2025**
 **New Delhi**

CHIEF GUEST
Dr Rabindra Narayan Behera
Hon'ble Member of Parliament, Lok Sabha



CKS Roundtable Discussion under the Aegis of Viksit Bharat.

Topic: Strengthening Data Protection for a Resilient Economy.

Theme: The Future of Data Protection and Policymaking in India: Balancing Innovation, Regulation, and National Security

Date: 19th May 2025

Venue: India Habitat Centre, New Delhi



Chief Guest Roundtable : 02



Centre for
Knowledge
Sovereignty®

VIKSIT BHARAT : DECODING THE DATA DILEMMA SOVEREIGNTY, STRATEGY & SECURITY IN THE AI AGE

Theme

**BUILDING DATA RESILIENCE AT SCALE : BALANCING INNOVATION,
REGULATION & NATIONAL SECURITY IN BHARAT'S DIGITAL DECADE**



12th August 2025



New Delhi

CHIEF GUEST

Shri. Sujeet Kumar

Hon'ble Member of Parliament, Rajya Sabha



CKS Roundtable Discussion under the Aegis of Viksit Bharat.

Topic: Decoding the Data Dilemma Sovereignty, Strategy & Security in the AI Age.

Theme: Building Data Resilience at Scale : Balancing Innovation, Regulation & National Security in Bharat's Digital Decade

Date: 12th Aug 2025

Venue: India Habitat Centre, New Delhi



Chief Guest Roundtable : 03



**Centre for
Knowledge
Sovereignty**

Presents Exclusive RoundTable on

**VIKSIT BHARAT : CYBER RESILIENCE & DATA PROTECTION,
A NATIONAL IMPERATIVE FOR CRITICAL INFRASTRUCTURE**

Theme

SECURING DATA, PROTECTING FUTURE, EMPOWERING A RESILIENT VIKSIT BHARAT

TUESDAY, 14TH OCT 2025
09:30AM | NEW DELHI

Chief Guest
Shri. Praveen K'Kumar
Managing Director
Dedicated Freight Corridor Corporation of India Ltd
A Govt of India (Ministry of Railways) Enterprise



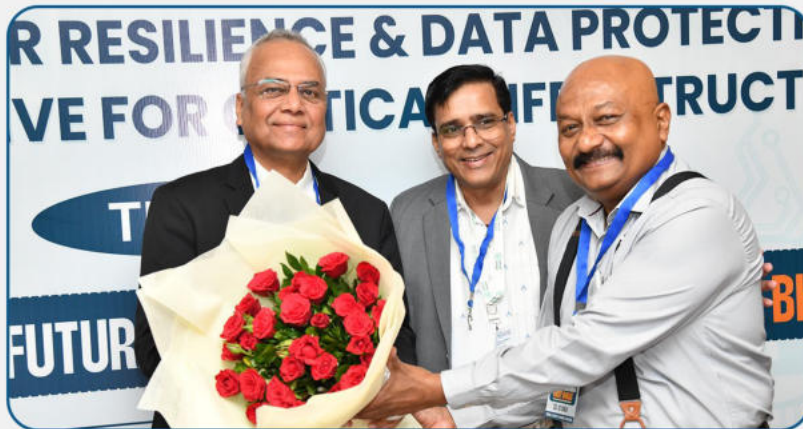
CKS Roundtable Discussion under the Aegis of Viksit Bharat.

Topic: Cyber Resilience & Data Protection, A National Imperative For Critical Infrastructure.

Theme: Securing Data, Protecting Future, Empowering A Resilient Viksit Bharat

Date: 14th Oct 2025

Venue: India Habitat Centre, New Delhi



Roundtable : 01



Roundtable : 02



Roundtable : 03





Participants

1. **Adv. Sujeet Kumar**- Hon'ble Member of Parliament, Rajya Sabha,
Member of Standing Committee on Science Technology, Environment, Forests and Climate Change
Member Consultative Committee for the Ministry of External Affairs, GOI.
Member Indian Council of World Affairs
Author of the book "AI on Trial"
2. **Dr. Rabindra Narayan Behera**- Hon'ble Member of Parliament, Lok Sabha
Member of Standing Committee of Communication and Information Technology
Member Consultative Committee of Steel Ministry, GOI.
3. **Mr. Praveen Kumar, IRSE**- Managing Director, Dedicated Freight Corridor Corporation of India Ltd
Ministry of Railways, GOI.
4. **Dr. C S Mohapatra, IES**- IEPF Chair Professor at NCAER, Fmr. Principal Adviser in the Rank of
Secretary to Govt of India, Fmr. Additional Secretary, Ministry of Finance, GOI.
5. **Prof. Dr. Unnat P Pandit**- Controller General of Patents, Designs and Trademark, (CGPDTM)
RoC, GI & SICLDR, GOI.
6. **Mr. Nitin Khade, IAS**- Joint Secretary, Department of Land Resources Ministry of Rural
Development, GOI.
7. **Major General Manjeet Singh, SM, VSM (Retd.)**- Joint Secretary- Cyber,
National Security Council Secretariat, (NSCS)PMO, GOI.
8. **Mr. Ajay Kumar Yadav, IPS**- Principal Resident Commissioner Govt of Himachal Pradesh
9. **Dr. Amit Sharma**- Additional Director General & Advisor (Cyber) Ministry of Defence, GOI.
10. **Mr. Sandeep Bhambure**- Vice President and Managing Director, Veeam India and SAARC
11. **Mr. Agendra Kumar**- Managing Director, Esri India
12. **Mr. Vinit Goenka**- Secretary, Centre for knowledge Sovereignty (CKS)
Author, Data Sovereignty The Pursuit of Supremacy
Fmr. Governing Council Member, CRIS, Ministry of Railways, GOI.
Fmr. Member IT Task Force, Ministry of Road Transport Highways and Shipping, GOI.
13. **Mr. Mahesh Jiwade, IRS**- Private Secretary to the Minister of State for Power and New &
Renewable Energy
14. **Mrs. Shubha N Bhambani, ITS**- Additional DGT, Department of Telecommunications, GOI.
15. **Mr. Amit Gunvant Bhole, ICAS**- DyCGA, Office of CGA Department of Expenditure Ministry
of Finance, GOI.
16. **Dr. G. Shreekumar Menon, IRS**- Fmr. Director General, National Academy of Customs,
Indirect Taxes & Narcotics, Ministry of Finance, GOI.
17. **Mr. Satya Narayan Meena, IRSSE**- Additional CEO & Chief Financial Officer Government
e-Marketplace (GeM), Ministry of Commerce & Industry GOI.
18. **Mr. Inder Pal Singh Sethi**- Fmr. Director General National Informatics Centre, GOI.
19. **Mr. Thirunarayanan Varadadesigan**- Principal Technical Program Mgr, Walmart Global Tech,
USA & Member CKS
20. **Mr. K B Nanda, IAS (Retd.)**- Fmr. Fin. Comm. Railway Board, Fmr. Principal Financial Advisor,
Northern Railway, North-Western Railway, Fmr. Executive Director Min. Of Railways, Fmr. Executive
Director Ircon International, Fmr. Director CCFB Railways Mozambique, Africa
21. **Mr. Manoj Tandon**- Director Project, Operations, Maintenance Railtel Corporation of India Ltd. GOI.
22. **Lt. Col. Alok Shankar Pandey**- Group General Manager/IT & Chief Information Security Officer
Dedicated Freight Corridor Corporation of India Limited, GOI.
23. **Mr. Pawan Kumar**- Executive Director (Finance) & Chief Compliance Officer Power Finance
Corporation Ltd. GOI.
24. **Dr Susil Kumar Meher**- Head Health IT and CISO AIIMS
25. **Mr. Keshri Kumar Asthana**- Chief Technology Officer, Public Sector, Microsoft India
26. **Mr. Jeevan Talegaonkar**- Vice President JIO Platforms Limited
27. **Mr. Ashok Narayanaswamy**- Chartered Accountant, Partner S.R.Batliboi & Co. LLP
28. **Mr. Amitava Sengupta**- President and Group Chief Digital Officer, RPSG Group
29. **Mr. S N Tripathi**- Executive Director, National Thermal Power Corporation

30. **Sumitra V Goenka**- Independent Director-Placda Infotech, Director-Madhyom Communications, CEO-Triangleglobal
31. **Mr. Vijay P. Karia**- Chairman and Managing Director of Ravin Group of Companies
32. **Lt. Gen. Vinod G. Khandare, PVSM, AVSM, SM (Retd.)**- Fmr. Principal Advisor, Ministry of Defence, GOI, and Fmr. Military Advisor NSCS, Fmr. DG Defence Intelligence Agency.
33. **Lt. Gen. Arun Kumar Sahni, PVSM, UYSM, SM, VSM (Retd.)**- Fmr. General Officer Commanding in Chief, Indian Army
34. **Mr. Jayadeva Ranade**- Fmr. Additional Secretary, Cabinet Secretariat
35. **Brigadier Aman Anand**- Indian Army
36. **Col. (Dr.) Anupam Tiwari, Ph.D.**- Advisor (Cyber) to Principal Advisor, MoD, Indian Army
37. **Commodore Naresh Chhabra**- DACIDS HQIDS, MoD
38. **Mr. Vijay Kumar**- Sr. Vice President and CTO, Esri India
39. **Col. VD Singh (Retd.)**- Fmr. Joint Director IT with DG Info System at Army HQ, Visiting Faculty at Institutes, Distinguished Fellow, CKS
40. **Col. Pankaj Awasthi (Retd.)**- Cybersecurity Leader
41. **Lt. Col. Nishant Singh (Retd.)**- VP & COO Gramax Cybertech
42. **Lt. Col. Amitabh Bhardwaj (Retd.)**- Director Projects – DST, IIT Madras
43. **Dr. Vijay Rai- Chief Business Strategist**- Governance, Resilience and Transformation, Veeam Software. & Distinguished Fellow-CKS
44. **Ms. Arundhati Bhowmick**- Group General Manager, HOD(IT) Engineering Projects INDIA Ltd. GOI.
45. **Mr. Basudeb Das**- Head of Department, NBO Ministry of Housing & Urban Affairs, GOI.
46. **Mr. Saurabh Jain**- Deputy Director, Infosecurity (ITBA), CBDT, GOI.
47. **Mr. Harvinder Kumar**- Deputy Director, Income Tax Ministry of Finance, GOI.
48. **Mr. Yogendra Prasad**- Assistant Director, Department of Telecom (DoT), GOI.
49. **Dr. Debapriya Dutta**- Fmr. Advisor of Department of Science and Technology, GOI.
50. **Mr. Sohan Nautiyal**- Principal Consultant Digital India Corporation, GOI.
51. **Mr. Vipul Srivastava**- IMC Chamber of Commerce and Industry
52. **Dr. Pankaj Vashist**- Associate Professor, RIS
53. **Mr. Santulan Chaubey**- Fmr. Jt. Director Department of Information Technology, Govt of Delhi
54. **Mr. Digvijaysinh Chudasama**- Partner, Deloitte India
55. **Mr. Eshwar Reddy Keesara**- Managing Director Dakkhin
56. **Dr. Ravindra Kumar**- Chief Scientist & Head ILT, CRRI, GOI.
57. **Mr. Mukesh Jain**- CTO & EVP, Capgemini
58. **Mr. Saket Setu**- CEO, Towards Vision Technologies limited (C-Zentrix)
59. **Mr. Rajesh Gupta**- Associate Head IT-Infrastructure and Security, Perfetti Van Melle
60. **Mr. Golok Kumar Simli**- President Technology & Innovation (Global) BLS International & Fmr. Principal Advisor & CTO, Passport Seva Program 2.0 & ePassport, GOI.
61. **Mr. Tapendra Dev**- Founder & CEO Of Secure Blink
62. **Mr. Kushagra Sharma**- Marketing Head, India & SAARC, Veeam
63. **Mr. Vivek Tiwari**- Founder and CEO, Audix Techno Consulting Solutions Pvt Ltd
64. **Mr. Pratham Vijay Karia**- Director, Ravin Group
65. **Mr. Viraj Chouhan**- Group Corporate Affairs Officer, RP Sanjiv Goenka Group
66. **Mr. Sanil Namboordiripad**- Fmr. Chief Operating Officer, Indigrid Investment Managers Limited
67. **Mr. Dr Anuranjan Misra**- Professor & Dean, Greater Noida Institute of Technology (GNIT)
68. **Mr. Krishan Dev Nidumolu**- Head Information Security, Insurance Information Bureau of India
69. **Manish Chaudhary**- Vice President Sales, Aathreya Labs Private Limited (ALABS)
70. **Ms. Anamika Das**- Head, Advocacy and Strategic Programs, ESRI India
71. **Mr. Manoj Gupta**- Senior General Manager, TeamLease Edtech
72. **Ms. Nischala Murthy Kaushik**- CMO, Opus Technologies
73. **Mr. Pulkit Chaudhary**- Data Privacy Expert & Legal Counsel, Sberbank
74. **Dr. Ashish Kumar**- Scientist 'C', CERT-In, Ministry of Electronics & Information Technology, GOI.
75. **Mr. Rishab Gulati**- Editor-in-Chief- NewsX & NewsX World
76. **Mr. Saurabh Sehgal**- Director, Sapphire International School Greater Noida
77. **Dr. Nagarathna A.**- Associate Professor, National Law School of India University Bengaluru
78. **Ms. Ekta Soni**- Assistant Director Academics and Principal, Sapphire International School

79. **Dr. Kriti Singh**- Honorary Advisor for Media Relations and Research, CKS
80. **Dr. Jinny Tomar**- Advocate, Delhi High Court, SCS Partners
81. **Ms. Anusha Soni**- Fmr. Editor, CNN News 18
82. **Mr. Naresh Kumar**- AGM, BSNL
83. **Dr. Satbir Yadav**- Fmr. DGM, CSD, Ministry of Defence, GOI.
84. **Mr. Swapan Biswas**- Consultant, CSC eGovernance Service, GOI.
85. **Mr. Yuvraj Chopra**- Country Advocacy Lead, Agri Solutions, BASF India Ltd
86. **Mr. Kawal Walia**- EVP, WalSof Technologies
87. **Wing Commander Deepak Prasad**- Indian Air Force
88. **Mr. Sanjay Sharan, IRS**- Fmr. Commissioner, Customs & CGST





Attendees



Sujeet Kumar

Hon'ble Member of Parliament, Rajya Sabha,
Member of Standing Committee on Science
Technology, Environment, Forests
and Climate Change,
Member Consultative Committee
for the Ministry of External Affairs, GOI.
Member Indian Council of World Affairs
Author of the book "AI on Trial"



Dr. Rabindra Narayan Behera

Hon'ble Member of Parliament, Lok Sabha,
Member of Standing Committee
of Communication and Information Technology,
Member Consultative Committee
of Steel Ministry, GOI.



Vinit Goenka

Secretary- Centre for knowledge
Sovereignty (CKS),
Author- Data Sovereignty The Pursuit
of Supremacy,
Fmr. Governing Council Member - CRIS,
Ministry of Railways, GOI,
Fmr. Member IT Task Force - Ministry of Road
Transport Highways and Shipping, GOI.



IRSE Praveen Kumar

Managing Director
Dedicated Freight Corridor Corporation
of India Ltd, Ministry of Railways, GOI.



Dr. C S Mohapatra, IES

IEPF Chair Professor at NCAER,
Fmr. Principal Adviser in the Rank of
Secretary Ministry of Finance GOI.



Nitin Khade IAS

Joint Secretary
Department of Land Resources
Ministry of Rural Development, GOI.



Prof. Dr. Unnat P Pandit

Controller General of Patents
Designs and Trademark, (CGPDTM)
RoC&GI, DPIIT MoC&I, GOI.



Major General Manjeet Singh

SM, VSM (Retd.) Joint Secretary- Cyber
National Security Council Secretariat,
(NSCS) PMO GOI.



Dr. Amit Sharma

Addl. Director General & Advisor (Cyber)
Ministry of Defence
GOI.



Ajay Kumar Yadav, IPS

Principal Resident Commissioner
Govt. of Himachal Pradesh



Sandeep Bhambure

Vice President and Managing Director
Veeam India and SAARC



Agendra Kumar

Managing Director
Esri India



Mahesh Jiwade, IRS

PS to Union Minister of State for Power and
New & Renewable Energy, GOI.



Shubha N Bhambhani (ITS)

Addl. DGT, Department of
Telecommunications, GOI.



Amit Gunvant Bhole, ICAS

DyCGA, Office of CGA
Department of Expenditure Ministry
of Finance, GOI.



Dr. G. Shreekumar Menon, IRS

Fmr. Director General, National Academy of
Customs, Indirect Taxes & Narcotics,
Ministry of Finance, GOI.



Satya Narayan Meena, IRSSE

Addl. CEO & CFO
Government e-Marketplace (GeM),
Ministry of Commerce & Industry, GOI.



Inder Pal Singh Sethi

Fmr. Director General
National Informatics Centre, GOI.



S N Tripathi

Executive Director
NTPC



K B Nanda, IRAS

Fmr. Addl. Member (Finance)
Railway Board, GOI.



Manoj Tandon

Director Project, Operations, Maintenance
Railtel Corporation of India Ltd. GOI.



Dr. Vijay Rai

Chief Business Strategist - Governance,
Resilience and Transformation, Veeam Software
& Distinguished Fellow - CKS



Vijay Kumar

Sr. Vice President and CTO
Esri India



Sumitra V Goenka

Independent Director-Plada Infotech,
Director - Madhyom Communications
CEO - Triangleglobal



Vijay P. Karia

Chairman and Managing Director of
Ravin Group of Companies



Lt. General Vinod Khandare

PVSM, AVSM, SM (Retd.)
Fmr. Principal Advisor MoD, Fmr. Military Advisor
NSCS, Fmr. DG Defence Intelligence Agency



Lt. General Arun Kumar Sahni

PVSM, UYSM, SM, VSM (Retd.)
Fmr. General Officer Commanding in Chief
Indian Army



Jayadeva Ranade

Addl. Secretary, Research &
Analysis Wing, Cabinet Secretariat



Commodore Naresh Chhabra

DACIDS, ICT Design, Directorate of ICT&N
Indian Navy



Brigadier Aman Anand

Indian Army



Col. (Dr.) Anupam Tiwari, Ph.D.

Advisor (Cyber) o/o Principal Advisor MoD
Visiting Faculty at Institutes, Indian Army



Col. VD Singh

Fmr. Joint Director IT with DG Info
System at Army HQ, Visiting Faculty at Institutes
Distinguished Fellow, CKS



Col. Pankaj Awasthi (Retd.)

Cybersecurity Leader



Lt. Col. Nishant Singh (Retd.)

VP & COO
Gramax Cybertech



Lt. Col. Amitabh Bhardwaj

Director Projects - DST, IIT Madras PTF



Lt. Col. Alok Shankar Pandey

Group General Manager-IT &
Chief Information Security Officer
Dedicated Freight Corridor Corporation of India Ltd.
GOI.



Pawan Kumar

Executive Director (Finance) &
Chief Compliance Officer
Power Finance Corporation Ltd. GOI.



Dr Susil Kumar Meher

Head Health IT and CISO
AIIMS



Arundhati Bhowmick

Group General Manager, HOD(IT)
Engineering Projects (INDIA) Ltd. GOI.



Basudeb Das

Director/HoD, National Buildings
Organisation (NBO), GOI.



Saurabh Jain

Deputy Director - Infosecurity
Income Tax Business Application (ITBA), GOI.



Harvinder Kumar

Deputy Director
Income Tax - CBDT, GOI.



Yogendra Prasad

Assistant Director
Department of Telecom (DoT), GOI.



Dr. Debapriya Dutta

Fmr. Advisor of Department of Science
and Technology, GOI.



Sohan Nautiyal

Principal Consultant
Digital India Corporation, GOI.



Vipul Srivastava

IMC Chamber of Commerce
and Industry



Dr Pankaj Vashisht

Associate Professor and Coordinator,
ASEAN-India Centre (AIC) at RIS



Santulan Chaubey

Fmr. Jt. Director Department of
Information Technology, Govt. of Delhi



Digvijaysinh Chudasama

Partner
Deloitte India



Ashok Narayanaswamy

Chartered Accountant
Partner S.R.Batlboi & Co. LLP



Amitava Sengupta

President and Group Chief Digital Officer
RP Sanjiv Goenka Group



Eshwar Reddy Keesara

Managing Director
Dakshin



Keshri Kumar Asthana

Chief Technology Officer – Public Sector
Microsoft India



Jeevan Talegaonkar

Vice President
JIO Platforms Limited



Dr. Ravindra Kumar

Chief Scientist & Head ILT
CRR, GOI.



Mukesh Jain

CTO & EVP
Capgemini



Saket Setu

CEO – Towards Vision Technologies
Limited (C-Zentrix)



Rajesh Gupta

Associate Head IT – Infrastructure
and Security, Perfetti Van Melle



Golok Kumar Simli

President Technology & Innovation (Global) BLS
International
Fmr. Principal Advisor & CTO Passport Seva
Program 2.0 & ePassport, GOI.



Tapendra Dev

Founder & CEO
Secure Blink



Kushagra Sharma

Chief Marketing Officer
Veeam



Vivek Tiwari

Founder & CEO – Audix Global (Audix
Techno Consulting Solutions Pvt Ltd)



Thirunarayanan Varadadesigan

Principal Technical Program Manager
Walmart Global Tech



Pratham Vijay Karia

Director
Ravin Group



Viraj Chouhan

Group Corporate Affairs officer
RP Sanjiv Goenka Group



Sanil Namboordiripad

Fmr. Chief Operating Officer
Indigrid Investment Managers Ltd.



Dr Anuranjan Misra

Professor & Dean at Greater Noida
Institute of Technology (GNIOT)



Krishan Dev Nidumolu

Head Information Security
Insurance Information Bureau of India



Manish Chaudhary

Vice President Sales Aathreya
Labs Private Limited (ALABS)



Anamika Das

Head – Advocacy and Strategic Programs
ESRI India



Manoj Gupta

Senior General Manager
TeamLease Edtech



Nischala Murthy Kaushik

CMO
Opus Technologies



Pulkit Chaudhary

Data Privacy Expert & Legal Counsel
Sberbank



Ashish Kumar

Scientist-C, ICERT
Ministry of Electronics and IT, GOI.



Rishabh Gulati

Editor-in-Chief
NewsX & NewsX World



Saurabh Sehgal

Director, Sapphire International
School Greater Noida



Dr. Nagarathna A.

Associate Professor of Law
National Law School of India
University, Bengaluru



Ekta Soni

Assistant Director Academics & Principal
Sapphire International School



Dr. Kriti Singh

Honorary Advisor for Media Relations
and Research, CKS



Dr. Jinny Tomar

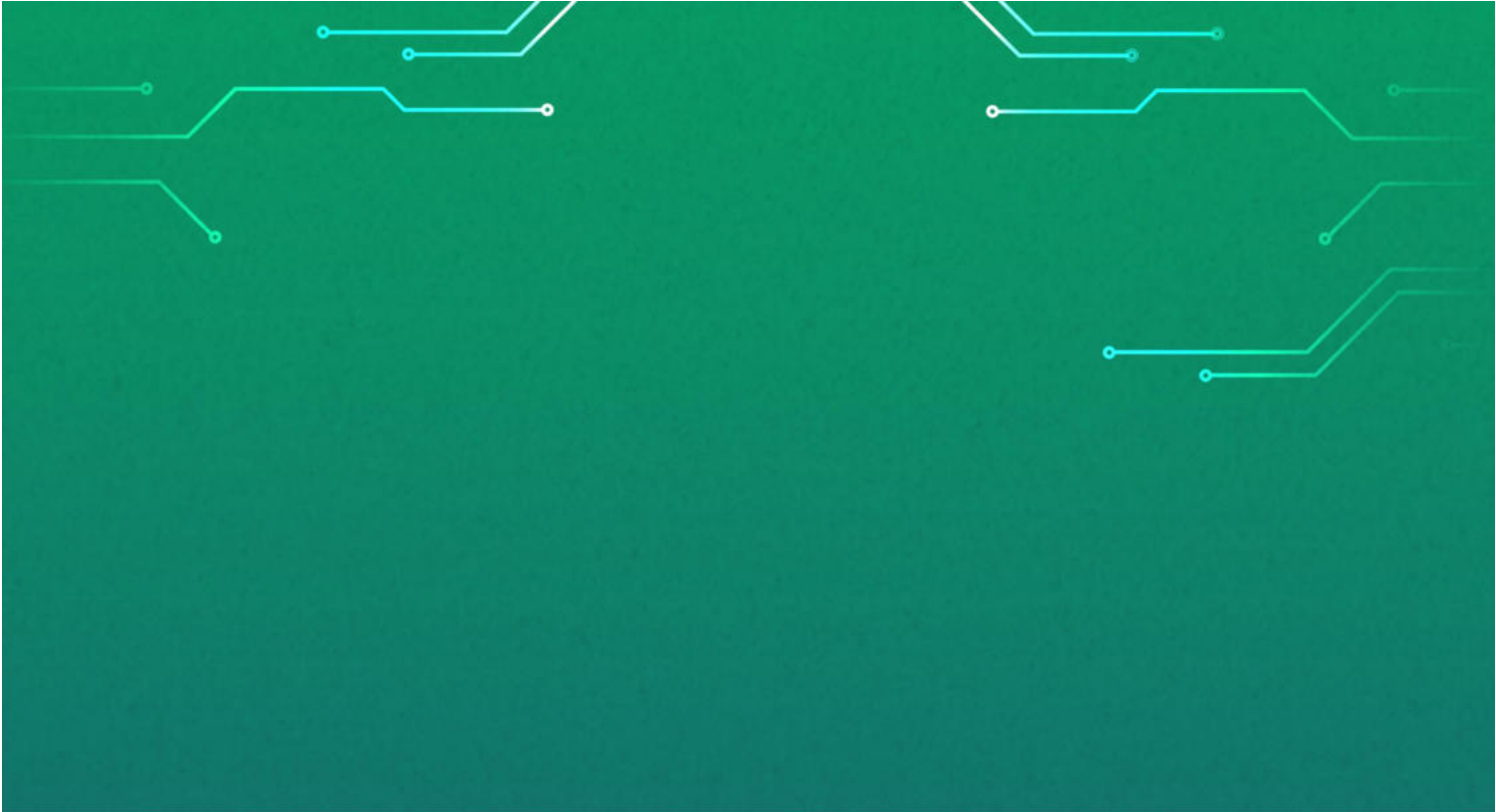
Advocate, Delhi High Court
SCS Partners



Anusha Soni

Fmr. Editor
CNN News 18

1. **Naresh Kumar**, AGM, BSNL
2. **Dr. Satbir Yadav**, Fmr. DGM, CSD, Ministry of Defence, GOI.
3. **Swapan Biswas**, Consultant, CSC eGovernance Service, GOI.
4. **Yuvraj Chopra**, Country Advocacy Lead, Agri Solutions, BASF India Ltd
5. **Kawal Walia**, EVP WalSof Technologies
6. **Wing Commander Deepak Prasad**, Indian Air Force
7. **Sanjay Sharan, IRS**, Fmr. Commissioner of Customs & CGST, GOI.

An abstract pattern of light blue and white lines resembling a circuit board, set against a dark green background. The lines are composed of horizontal, vertical, and diagonal segments, with small circles at the endpoints, creating a sense of digital connectivity.

Report on Data Resilience in India: A Framework for National Digital Security

An abstract pattern of light blue and white lines resembling a circuit board, set against a dark blue background. The lines are composed of horizontal, vertical, and diagonal segments, with small circles at the endpoints, creating a sense of digital connectivity.

Contents

Report on Data Resilience in India: A Framework for National Digital Security.....	1
Abbreviations List.....	3
Executive Summary	6
Introduction.....	9
Methodology.....	13
Sources and Research Process.....	13
Findings.....	28
The Evolution of Digital Colonization	28
India's Current Threat Landscape	28
Data Resilience and Business Continuity	38
Technology Dependencies and Indigenous Capabilities.....	41
The Human Factor and Capacity Building	43
Emerging Technologies: Opportunities and Threats.....	44
Institutional Framework and Governance.....	45
Vision 2047 and the Path Forward	47
Analysis.....	50
India's Current Data Resilience Posture.....	50
Gaps and Vulnerabilities.....	52
International Comparisons and Best Practices.....	54
Need for a National Data Resilience Doctrine.....	57
Implementing the DPDP Act.....	58
Recommendations.....	59
Strategic Priorities and Immediate Actions	60
Strengthening Data Protection Infrastructure	65
Policy and Regulatory Framework	68
Building National Capacity	69
Implement Resilience Metrics and Maturity Model Framework.....	72
Conclusion	74
Endnotes.....	75

Abbreviations List

AI - Artificial Intelligence

AIIMS - All India Institute of Medical Sciences

BCP - Business Continuity Planning

BFSI - Banking, Financial Services, and Insurance

BIA - Business Impact Analysis

BNS - Bharatiya Nyaya Sanhita

BSNL - Bharat Sanchar Nigam Limited

BYOVD - Bring Your Own Vulnerable Driver

CERT-In - Indian Computer Emergency Response Team

CISO - Chief Information Security Officer

CKS - Centre for Knowledge Sovereignty

CSA - Cyber Security Agency (Singapore)

CSIRT-Fin - Computer Security Incident Response Team - Financial Sector

CSIRT-Power - Computer Security Incident Response Team - Power Sector

DFCCIL - Dedicated Freight Corridor Corporation of India Limited

DPI - Digital Public Infrastructure

DPDP - Digital Personal Data Protection

EDR - Endpoint Detection and Response

EU - European Union

FASTag - Electronic Toll Collection System

GCI - Global Cybersecurity Index

GDP - Gross Domestic Product

GDPR - General Data Protection Regulation

GCHQ - Government Communications Headquarters (UK)

GLBA - Gramm-Leach-Bliley Act

GRC - Governance, Risk, and Compliance

HIPAA - Health Insurance Portability and Accountability Act

I4C - Indian Cyber Crime Coordination Centre

ICS-CERT - Industrial Control Systems Cyber Emergency Response Team

IIT - Indian Institute of Technology

IIM - Indian Institute of Management

IRDAI - Insurance Regulatory and Development Authority of India

ISAC - Information Sharing and Analysis Center

ISO - International Organization for Standardization

ISRO - Indian Space Research Organisation

IT - Information Technology

ITU - International Telecommunication Union

JNPT - Jawaharlal Nehru Port Trust

LOLBins - Living-Off-the-Land Binaries and Scripts

MEITY - Ministry of Electronics and Information Technology

MMGIS - Master Mentor Geospatial Enabling Indian Students

MTD - Mean Time to Detect

MTR - Mean Time to Return/Respond

NCIIPC - National Critical Information Infrastructure Protection Centre

NCSC - National Cyber Security Centre (UK)

NDRA - National Data Resilience Authority (Proposed)

NEFT - National Electronic Funds Transfer

NIST - National Institute of Standards and Technology (USA)

NPCI - National Payments Corporation of India

OECD - Organisation for Economic Co-operation and Development

OT - Operational Technology

PAN - Permanent Account Number

PC - Personal Computer

PIPL - Personal Information Protection Law (China)

PMO - Prime Minister's Office

RBI - Reserve Bank of India

RMM - Remote Monitoring and Management

RPO - Recovery Point Objective

RTGS - Real Time Gross Settlement

RTO - Recovery Time Objective

SaaS - Software as a Service

SEBI - Securities and Exchange Board of India

SIM - Subscriber Identity Module

SQL - Structured Query Language

SWIFT - Society for Worldwide Interbank Financial Telecommunication

TRAI - Telecom Regulatory Authority of India

UK - United Kingdom

UN - United Nations

UPI - Unified Payments Interface

USA/US - United States of America

USD - United States Dollar

Executive Summary

India's impressive digital transformation over the last decade has made the country a global technology leader. While this rapid digital growth drives economic development and social inclusion, it also introduces new vulnerabilities that need immediate attention. The scale of India's digital infrastructure, which supports over a billion citizens and processes trillions of rupees in annual transactions, has made it a prime target for advanced cyber threats. This situation has turned data resilience from a technical issue into a crucial matter of national security and economic stability.

This report is based on three roundtable discussions organized by the Centre for Knowledge Sovereignty from May to October 2025. It gathers insights from more than 100 experts from government agencies, military leaders, company executives, parliamentarians, academic institutions, and cybersecurity professionals. The discussions reveal a complex and worsening threat landscape characterized by increased frequency, sophistication, and geopolitical dimensions of cyberattacks targeting India's critical infrastructure, financial systems, personal data, and government operations. The geopolitical situation adds to these concerns.

India faces significant vulnerabilities across three interconnected areas. First, there are geopolitical dependencies in digital infrastructure. This puts the nation at risk of potential weaponization by foreign actors. Second, the threat of ransomware is increasing, with complex, multi-stage extortion methods employed. Lastly, both public and private sectors show systemic weaknesses in data security. These gaps have led to major breaches impacting millions of citizens and causing significant financial losses. These issues highlight the urgent need for improved digital sovereignty and stronger cybersecurity measures at the national level.

The report points out significant vulnerabilities in India's essential infrastructure. India's critical infrastructure faces ongoing cyber threats in various sectors. Essential services systems are continually subjected to attack attempts that exploit both operational gaps and technical weaknesses. The cybersecurity stance is weakened by a basic architectural issue. Legacy operational technology systems in strategic sectors were designed decades ago without considering security. They also run on very different update schedules compared to modern IT infrastructure, which creates ongoing exposure. At the same time, the nation's ambitious digital transformation efforts are improving operational efficiency but are also unintentionally broadening the attack surface.

This digitization of sensitive infrastructure data could be used for targeted attacks, creating a national security dilemma where modernization efforts might make us more vulnerable instead of less. India's critical infrastructure faces ongoing cyber threats in various sectors. The cybersecurity stance is weakened by a basic architectural issue.

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

India is facing a shortage of cybersecurity professionals, which severely hampers its capacity to secure its expanding digital infrastructure. This shortage appears in several areas: not enough trained personnel, a lack of specialized expertise in crucial fields, and a dearth of strategic leaders who can connect technical needs with business and policy contexts. Chief Information Security Officer positions often serve as part-time roles for bureaucrats rather than full-time certified professionals, leading to inconsistent competencies in key roles. The professionalization of cybersecurity roles lacks the development seen in medical or legal fields that require ongoing education and certifications.

Reliance on foreign technology creates weaknesses that adversaries can exploit during conflicts or diplomatic tensions. The lack of homegrown operating systems, domain name systems, and complete geographical information systems means adversaries might be able to take control of, or compromise, the technology supporting India's digital ecosystem. Even when data is hosted within India, operational control often remains overseas via foreign software platforms, management dashboards, and administrative access. The absence of domestic artificial intelligence models suited to Indian needs, languages, and requirements increases dependence on systems created elsewhere, which may reflect different values, priorities, and inherent vulnerabilities.

Coordination issues among various regulatory bodies viz. CERT-In, NPCI, SEBI, RBI, TRAI, and specific sector regulators, lead to fragmented requirements that organizations find challenging to navigate. Rules for cross-border data transfers remain vague, with unpublished restricted country lists complicating international operations, especially for startups and small businesses. The decentralized nature of India's digital infrastructure, where each department controls its IT and cybersecurity frameworks, results in varied capabilities and inconsistent protections across sectors.

Despite these challenges, India has made significant progress that deserves recognition. India has gained considerable recognition in global cybersecurity rankings, showing both strong institutions and operational readiness through internationally recognized frameworks and practices. The country has demonstrated its ability to defend against large, complex cyber-attacks through coordinated responses that use advanced technologies to create credible deterrence. Additionally, India's Digital Public Infrastructure is a key asset that combines technical expertise in managing high-volume, critical systems with resilience, making the country a model for digital economy architecture. These abilities are backed by a developing network of specialized response teams and coordination centers that support strategic-level management of cyber incidents across different sectors.

The report offers detailed recommendations divided into strategic priorities that require immediate action, including strengthening data protection infrastructure, improving policy and regulatory frameworks, and expanding national capacity building. A Data Resilience Doctrine would provide the unifying framework currently absent, establishing clear command structures, standardized protocols, and unified metrics across all critical infrastructure sectors. Unlike the National Cybersecurity Policy 2013, which remains aspirational mainly and outdated, a doctrine represents actionable military-grade planning that defines roles, responsibilities, escalation procedures, and response mechanisms with precision.

Key immediate steps involve setting up a unified National Data Resilience Authority to address fragmentation among agencies, launching a mission-mode quantum-safe cryptography program to counter new threats, and requiring thorough security audits for all critical infrastructure operators with certification needed. Infrastructure recommendations include establishing distributed national data centers with geographic spread, developing domestic cloud infrastructure and operating systems through a National Indigenous Technology Mission, creating sector-specific data trusts for information sharing, and implementing zero trust architecture for government networks by 2028.

Policy and regulatory priorities involve finalizing the Digital Personal Data Protection Act's implementation with an empowered Data Protection Board within six months, creating a unified compliance framework that integrates several regulations to lessen the organizational burden, publishing lists of restricted countries and frameworks for cross-border transfers to clarify legal issues, and requiring cybersecurity professional certification for crucial roles with ongoing education obligations.

Reaching Viksit Bharat Vision 2047 requires India to turn current vulnerabilities into future strengths through ongoing commitment, significant resources, and collaboration among government, industry, academia, and civil society. This investment is both urgent and essential. The choices made today will shape whether India realizes its goal of becoming a five trillion-dollar economy by 2027, and possibly a 30 trillion dollar economy by 2047, or if it faces challenges from technological dependencies, skills shortages, and infrastructure weaknesses that can hinder economic growth and strategic independence.¹ Achieving success requires viewing data resilience not just as a technical issue for specialists but as a national priority that calls for the engagement of the entire society with resources that match the stakes of securing India's digital future.

Introduction

The past decade has seen India rise as a major digital powerhouse. Over the past decade, digital-enabling industries have grown at a rate of 17.3%, notably outpacing the 11.8% growth recorded by the overall economy.² In 2022–23, the digital economy employed approximately 14.67 million people, representing 2.55% of India's total workforce.³ Digital infrastructure has come to support economic growth, government services, and social inclusion. The Digital India Mission, launched in 2015, has not only improved technology but has also fundamentally changed how over a billion citizens engage with the government, the economy, and one another.

The journey of digital acceptance in India shows a remarkable pace of change. Internet subscribers increased from 251.59 million in March 2014 to 954.40 million in March 2024, reflecting a compound annual growth rate of 14.26 percent.⁴ The Unified Payments Interface, a key symbol of India's digital shift, now handles 83 percent of the nation's digital payment volume, up from 34 percent in 2019, positioning India as a leader in global real-time payments, accounting for 49 percent of worldwide transactions.⁵

The Digital India Mission has progressed through distinct phases, each building on prior foundations while expanding its objectives. It aimed initially to ensure basic digital access and inclusion by developing infrastructure. Aadhaar became its central identifier, providing biometric-based digital identities to over 1.42 billion residents of India, representing 97 percent of the national population.⁶

This digital identity infrastructure enabled direct benefit transfers that have saved the government an estimated 3.48 lakh crore rupees by eliminating fraudulent beneficiaries. At the same time, platforms such as DigiLocker now serve over 300 million users with 6.75 billion issued.⁷ The Digital India Mission has subsequently shifted toward integrated, citizen-focused service delivery. It is now in a phase that prioritises future readiness through emerging technologies like artificial intelligence, blockchain, and the Internet of Things.

Infrastructure growth has been key to this digital change, with the BharatNet project, one of the world's most significant rural telecommunications initiatives, having made 2.13 lakh Gram Panchayats ready for service with optical fiber connectivity, out of a target of 2.22 lakh.⁸ As of April 2024, 95.15 percent of India's 644,131 villages now have access to 3G or 4G mobile connectivity.⁹

The economic effects of India's digital transformation extend far beyond infrastructure numbers. The country's digital economy accounted for 11.74% of the GDP (INR 31.64 lakh crore or USD 402 billion) in 2022–23, employing 14.67 million workers (i.e. 2.55% of the workforce).¹⁰ Research by McKinsey suggests that the Digital India initiative could increase the country's digital economy to \$1 trillion by 2025. The Digital Public Infrastructure, exemplified by Aadhaar, UPI, and other platforms, has become a global model, attracting attention from other nations looking to replicate India's success in using technology for inclusive growth.

India has emerged as a formidable participant in the global data economy, ranking third worldwide in terms of economy-wide digitalisation, behind only the United States and China.¹¹ This

positioning reflects not merely the country's technological infrastructure but also its transformation into a data-intensive economy in which digital processes increasingly drive value creation across traditional and emerging sectors.

The scale of India's digital economy commands attention both domestically and internationally. The maturation of India's digital ecosystem is evident in specific technology segments experiencing rapid growth. The public cloud services market is projected to reach thirteen billion dollars by 2026, expanding at a compound annual growth rate of 23.1 percent, reflecting enterprise adoption of scalable digital infrastructure.¹²

Data center capacity, fundamental to supporting digital operations, stood at 950 megawatts as of 2024 with projections indicating an additional 850 megawatts by 2026, positioning India as a significant participant in the Asia-Pacific data center landscape.¹³ The telecommunications sector, having successfully deployed extensive 4G coverage, is now implementing 5G networks in major urban centers, with plans for broader rollout to support advanced applications in telemedicine, autonomous systems, and industrial automation.¹⁴

Despite these achievements, India's integration into global data flows reveals persistent regulatory complexity that affects its position in international digital trade. The country has implemented sector-specific data localization requirements across payments, insurance, telecommunications, and other domains, reflecting concerns about data sovereignty, security, and local value creation.¹⁵

While the Digital Personal Data Protection Act establishes a comprehensive framework for cross-border data transfers, allowing such transfers subject to government approval and restricted country lists yet to be notified, regulatory uncertainty persists regarding implementation details.¹⁶ This regulatory approach attempts to balance participation in global digital value chains with protection of national interests, though the effectiveness of this balance remains subject to ongoing assessment.

India's advancement toward digital sovereignty reflects broader global trends wherein nations seek greater control over data flows, technology standards, and digital infrastructure within their jurisdictions. The Organisation for Economic Co-operation and Development (OECD) has documented that restrictive cross-border data policies, while often motivated by legitimate privacy and security concerns, can impose substantial costs, with data localization measures potentially raising data management expenses by fifteen to fifty-five percent.¹⁷

For India, which simultaneously serves as a major exporter of digital services and an expanding market for global technology platforms, crafting policies that enable beneficial data flows while protecting national interests remains an ongoing challenge with significant economic implications.

This digital transformation creates new vulnerabilities that need urgent attention. The collection of sensitive personal and financial data within digital systems, the use of essential services that rely on internet platforms—like healthcare and education—and the rise of digital payment systems handling trillions of rupees each year all attract malicious actors.¹⁸

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y
C
E
N
T
R
E

With Aadhaar authentication transactions exceeding 2,707 crore in fiscal year 2024-25, and face authentication alone processing over fifteen crore transactions in March 2025, the amount of sensitive biometric and demographic data in circulation has reached new heights. The Ministry of Electronics and Information Technology identifies this data as crucial for the digital economy and stresses the need for strong protection.¹⁹

Cyber threats targeting India's digital infrastructure have become increasingly sophisticated as the digital infrastructure has grown, creating an ongoing struggle between attackers and defenders. Official data shared with Parliament by the Ministry of Electronics and Information Technology reveals that the Indian Computer Emergency Response Team dealt with 1,391,457 cybersecurity incidents in 2022.²⁰

Among these, vulnerable services accounted for 875,892 incidents, highlighting systems that can leak data or be manipulated by external threats. This figure reflects both improved detection and a real increase in threats.

Phishing attacks rose by 230 percent compared to 2021; malware attacks increased by 45 percent, and incidents involving vulnerable services grew by 20 percent.²¹ However, India faces an estimated shortfall of around eight lakh cybersecurity professionals needed to defend against these more complex attacks.

The World Economic Forum highlights the seriousness of this gap, noting that 30% of India's 40,000 cybersecurity job openings in May 2023 remained unfilled, despite India having nearly one-third of the world's science, technology, engineering, and mathematics graduates.²²

Ransomware attacks, data breaches, and advanced cyber espionage operations are not just about financial gain; they pose strategic threats that can affect economic stability and national security. The interconnected nature of India's Digital Public Infrastructure means that weaknesses in one system can impact multiple services, significantly increasing potential damage from successful attacks.

The National Critical Information Infrastructure Protection Centre continuously monitors this risk as the leading agency responsible for protecting critical information infrastructure.²³ A statement from the Ministry of Electronics and Information Technology, issued in February 2025, acknowledges that the rapid digital transformation of the financial sector has created cyber risks with far-reaching effects on economic stability and public trust.²⁴ This situation calls for coordinated efforts across the entire government rather than disjointed responses from various sectors.

Data resilience is therefore essential for national security and economic independence, rather than just a technical issue within information technology. As India's digital economy aims to contribute one-fifth of national income by 2029-30 and enhances its role in global data flows—leading in real-time payment transactions and IT service exports—the ability to protect data, ensure system availability, and maintain citizen trust is crucial to sustaining the country's digital growth.

The frameworks and strategies developed to address data resilience challenges will determine whether India's digital transformation continues to drive inclusive growth and strategic advantages, or becomes a point of vulnerability that adversaries might exploit for economic disruption or coercion. This report reviews the current state of data resilience in India, examines the various threats facing the digital ecosystem, identifies gaps in existing protections, and suggests ways to strengthen national digital security in line with both the country's ambitions and the scale of vulnerabilities its success has created.



Methodology

The need for data resilience in India's digital ecosystem stems from rapid digital adoption, rising cyber threats, and recognition that data infrastructure is critical national infrastructure that must be protected, analogous to physical infrastructure that secures territorial sovereignty.

This section examines the foundational concepts, analytical frameworks, and policy needs that define data resilience as crucial to supporting India's digital transformation while safeguarding national security and economic interests.

The approach in this report integrates regulatory frameworks, threat assessments, institutional capacity evaluations, and policy comparisons to develop a comprehensive understanding of the specific data-resilience needs within India's development context and security landscape.

Data resilience, as discussed in this report, extends beyond traditional cybersecurity approaches that primarily focus on threat prevention. It encompasses the broader capacity of digital ecosystems to anticipate, withstand, contain, recover from, and adapt to disruptions that affect data integrity, availability, or confidentiality.

Data resilience is defined as the organizational and national capability to maintain continuous access to critical data assets, rapidly recover from cyber incidents or infrastructure failures, and adapt systems to evolving threats while preserving data sovereignty and supporting India's strategic autonomy in an increasingly digitalized economy.

The Securities and Exchange Board of India's Cybersecurity and Cyber Resilience Framework, launched in August 2024, outlines this broad approach through five main functions: anticipate, withstand, contain, recover, and evolve.²⁵

This framework, developed with input from Market Infrastructure Institutions, regulated entities, industry groups, and government organizations, including the Indian Computer Emergency Response Team and the National Critical Information Infrastructure Protection Centre, offers a structured way to assess and improve cyber resilience across India's financial sector.²⁶

The emphasis on resilience over security reflects a growing understanding that, in complex, interconnected digital systems, preventing all threats is not feasible. Therefore, systems must be designed to keep essential functions running even when compromised and to recover quickly from successful attacks.²⁷

Sources and Research Process

Roundtable Consultations

The main foundation of this report comes from three roundtable discussions held by the Centre for Knowledge Sovereignty (CKS) between May and October 2025. These discussions included about 70 experts, practitioners, and policy stakeholders who focused on data sovereignty, cyber resilience, and protecting critical infrastructure in India.

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

The first roundtable took place on May 19, 2025. Its theme was "The Future of Data Protection and Policy Making In India- Balancing Innovation Regulation and National Security." This initial session set the stage for further discussions and identified significant gaps in India's cyber security framework. The second roundtable, held on August 12, 2025, was titled "Building Data Resilience at Scale: Balancing Innovation, Regulation & National Security in Bharat's Digital Decade." It looked at how emerging technologies intersect with national security needs. The third and final roundtable titled 'Cyber Resilience and Data Protection, A National Imperative for Critical Infrastructure occurred on October 14, 2025, and combined insights from earlier sessions while addressing new geopolitical threats and technological challenges.

Each roundtable included 20 to 25 selected participants representing a range of viewpoints. Participants across the three roundtables included incumbent Lok Sabha and Rajya Sabha Members of Parliament from key Standing and Consultative Committees; Joint Secretary and Additional Secretary-level officials across Ministries of Defence, Finance, Railways, Communications, and Electronics & IT; senior PSU leaders from NTPC, RailTel, BSNL, AIIMS, and Dedicated Freight Corridor Corporation; former Railway Board members, NIC Directors General, and Secretaries-rank advisors; serving and retired flag-rank military officers; CXOs from leading technology, cloud, and cybersecurity firms; industry representatives from chambers of commerce; academics, deans, and think-tank fellows; data protection counsel and CERT-In officials; and senior media editors and education leaders. The aim was to have a well-rounded representation of people involved in critical national infrastructure.

The process of organizing the roundtables followed a structured method for gathering information and engaging stakeholders. CKS maintains ongoing involvement with government policy developments, tracking legislative actions, policy proposals, and changes in strategic doctrines. If there are signs that the government is looking into specific policies related to data sovereignty, cyber security, or critical infrastructure, CKS starts planning roundtables.

Identifying participants involved a careful selection process that prioritizes expertise and diversity over rank alone. CKS seeks individuals who have practical experience, not just theoretical knowledge. This focus keeps discussions tied to real-world practices, rather than abstract ideas.

Invitations went 2 to 3 weeks before each roundtable. Participants receive general themes but no set agendas. This setup promotes a natural flow of discussion while sticking to relevant topics. Venues are chosen in the National Capital Region, often at neutral locations that support confidential conversations. The India Habitat Centre hosted several sessions, providing suitable facilities for large and small discussions.

All roundtable discussions followed modified Chatham House Rules. This allowed for open dialogue while protecting personal and institutional interests. Participants are advised that their inputs reflect personal views, not their organizations' positions. This is crucial for government

officials, military members, and corporate executives who may face restrictions when discussing sensitive issues.

Each speaker is given a strict time frame of 4 to 5 minutes for opening presentations. This rule serves several purposes: it ensures equal participation among the 20-25 speakers over a manageable timeframe (usually 3-4 hours per roundtable), it keeps contributions focused and concise, it prevents one perspective from dominating, and it allows for interaction after the initial talks.

- **Roundtable 1** (19 May 2025, “Strengthening Data Protection for a Resilient Economy”):
Chief Guest: Dr. Rabindra Narayan Behera, Hon’ble Member of Parliament, Lok Sabha.
- **Roundtable 2** (12 August 2025, “Decoding the Data Dilemma, Sovereignty, Strategy & Security in the AI Age”):
Chief Guest: Shri Sujeet Kumar, Hon’ble Member of Parliament, Rajya Sabha.
- **Roundtable 3** (14 October 2025, “Cyber Resilience & Data Protection, A National Imperative for Critical Infrastructure”):
Chief Guest: Shri Praveen Kumar, IRSE, Managing Director, Dedicated Freight Corridor Corporation of India Ltd, Ministry of Railways, Government of India.

After the initial presentations, moderated discussions enable clarification, challenge, and synthesis. Participants often built on each other's insights, contributing to a collective knowledge development rather than a series of separate talks. The Chair for the second roundtable, Dr. C.S. Mohapatra, Chair Professor Investor Education and Protection Fund, National Council of Applied Economic Research. Former Additional Secretary GST Council Secretariat, Department of Revenue, Ministry of Finance, noted that "ideas converge at a particular point," highlighting how different viewpoints coalesced around common concerns.

Documentation and Validation

Each roundtable session is recorded with participants' consent. Professional transcribers convert these recordings into verbatim text, capturing the exact language used, including pauses and interactions. These transcripts create the main documentary record, along with written submissions from participants who couldn't finish their thoughts during the discussion.

CKS researchers synthesize the transcript content, identifying recurring themes, new insights, areas of agreement and disagreement, technical points needing more investigation, and policy recommendations arising from the group discussions. This synthesis goes through several drafts, sharing sections with participants for fact-checking and accuracy verification.

The validation process respects Chatham House Rules. Participants review content based on their contributions for accuracy but do not approve or reject how their insights fit into the broader analysis. This maintains the research's independence while ensuring it remains reliable. Some participants provided additional written materials to expand on points that were too brief due to time limits, enriching the evidence base beyond just oral presentations.

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

The commemorative booklet published after the May, August and October 2025 roundtables includes participant lists, organizational affiliations, and summary observations. This adds transparency about who contributed to the knowledge generation while keeping specific attributions discreet. The booklet also serves as an accountability tool, showing the range and quality of expertise that informed CKS analysis.

Documentary and Open-Source Research

While roundtable consultations provide primary data, this report also includes significant secondary sources to place expert insights in a wider policy, technical, and strategic context.

Government documents include published legislation, especially the Digital Personal Data Protection Act, 2023, and related draft rules. They also cover policy frameworks and white papers from the Ministry of Electronics and Information Technology, the Ministry of Home Affairs, the Ministry of Defence, and other relevant ministries. Additionally, there are national cyber security strategies and advisories from agencies like the National Cyber Security Coordinator, parliamentary committee reports on information technology and data protection, and regulatory guidelines from bodies like the Reserve Bank of India and the Telecom Regulatory Authority of India.

Official documents provide clear government intentions, regulatory requirements, and institutional setups. However, as roundtable participants pointed out, there can be significant gaps between what is documented and what happens in practice. Secondary sources then help understand official frameworks, while primary sources highlight real-world situations.

Trustworthy media coverage of cyber security incidents, data breaches, and technology trends adds depth to technical and policy documents. Sources include established national newspapers, specialized technology and security magazines, and investigative journalism from respected outlets. Media reports proved useful for following specific incidents discussed during the roundtables, like the September 2022 ransomware attack on AIIMS Delhi and the Nayara Energy cloud access disruption.

Journalistic sources require careful evaluation given varying levels of accuracy and potential sensationalism. CKS researchers cross-checked media reports against accounts from roundtable participants, especially from those directly involved in the incidents. When discrepancies arose between media narratives and expert views, the latter were prioritized given the firsthand knowledge these participants had.

Reports from credible think tanks and research organizations focused on cyber security, data governance, and technology policy provided valuable context. Sources include reports from Indian institutions and international organizations.

Think tank publications often combine academic rigor with practical relevance, filling gaps not covered in government documents or media reports. However, researchers must consider the

perspectives and funding sources of these institutions to evaluate neutrality and completeness. CKS prioritized sources that showed methodological clarity and a solid empirical basis over ones focused on advocacy.

The corporate technology sector generates extensive research on cyber security threats, data protection practices, and resilience strategies. Sources include threat intelligence reports from key cyber security firms like Palo Alto Networks and Deloitte, industry surveys on security postures and incident responses, technical papers on specific vulnerabilities, and standards documentation from organizations like the International Organization for Standardization.

Commercial sources offer useful technical insights and trend analysis based on global incident tracking and surveys. However, researchers must critically assess vendor interests when considering these sources. When commercial sources informed the analysis, CKS sought validation from independent sources or through participant input during roundtable discussions.

The methodology combines primary roundtable insights with secondary research through thematic analysis. Initial coding of transcripts highlighted recurring topics, concerns, and recommendations from the three roundtables. Secondary sources then offered context and validation for these themes. In cases where primary and secondary sources differed, this report prioritizes insights from roundtable participants due to their practical experiences while acknowledging other viewpoints from documentary sources.

This mixed-methods approach, which combines expert consultations with documentary analysis, allows for a thorough examination of India's data resilience challenges. The roundtable discussions reveal gaps in implementation, organizational barriers, and emerging threats that formal documents may overlook, while secondary sources provide authoritative reference points and broader context that presentations alone cannot fully cover.

The resulting analysis integrates practical knowledge from those managing India's critical digital infrastructure, policy insights from government officials shaping regulations, strategic views from security professionals countering advanced threats, and technical expertise from specialists in cyber security and data protection. This comprehensive evidence base supports the observations, assessments, and recommendations in the following sections of this report.

This framework provides a structured approach for identifying threats to digital infrastructure, assessing which systems and data are vulnerable, and evaluating weaknesses that could be exploited. It helps pinpoint critical points in India's Digital Public Infrastructure where disruptions could impact multiple services, affecting millions of users and potentially destabilizing economic functions. For example, platforms such as Aadhaar, which processes over 2,707 crore transactions each year, demonstrate that weaknesses in authentication systems can expose all services that rely on Aadhaar verification, including banking, telecommunications, and government benefits.²⁸

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

Second, the report applies capability assessment methods to evaluate institutional, technical, and human resource aspects of data resilience. The Ministry of Electronics and Information Technology's establishment of the National Centre of Excellence in Cyber Security, in collaboration with the Data Security Council of India, underscores the government's recognition that developing domestic capabilities is essential to data resilience.²⁹

Although 12,014 officials were trained through 23 CERT-In programs in 2024, this capacity-building progress is insufficient to close the gap.³⁰

Third, the report employs comparative regulatory analysis to situate India's data governance frameworks within the global context of data sovereignty, data localization, and cross-border data flows. On May 26, 2022, the Ministry of Electronics and Information Technology released the Draft National Data Governance Framework Policy, which proposes standardizing data management across government entities and creating an India Datasets program to promote digital governance and stimulate AI and data-led innovation.³¹

This framework, still being finalized, seeks to address inconsistent data management practices across government departments while providing researchers and startups with access to anonymized non-personal datasets, balancing open data principles with security needs. The methodology looks at how India's approach, including sector-specific data localization rules across payments, insurance, and telecommunications, compares with other regulatory models, such as the European Union's General Data Protection Regulation and the practices of countries like Singapore and Australia that focus on data portability and facilitating international data flows.³²

Analyses of incident reports, financial loss metrics, and threat trend assessments from government and credible international sources clearly demonstrate the necessity of data resilience. In 2024, Indian citizens suffered losses of Rs.22,845.73 crore due to cyber fraud, a staggering 206 percent increase from the previous year's losses of Rs.7,465.18 crore.³³

These figures, presented to Parliament by the Ministry of Home Affairs, clearly highlight the economic impact of poor data resilience. However, they only capture direct financial theft reported through national cybercrime portals and do not consider productivity losses, remediation expenses, intellectual property theft, or loss of trust in digital systems.

The Banking, Financial Services, and Insurance sector faced intense targeting, with data breach costs in India reaching 2.18 million dollars per incident in 2024, a 28 percent increase over three years, according to the Digital Threat Report 2024 released by CERT-In, CSIRT-Fin, and SISA.³⁴

The methodology includes a threat landscape analysis that demonstrates that data resilience needs are dynamic and require adaptable defense strategies. India was identified as the main global target for mobile malware attacks in 2024, accounting for 28 percent of worldwide incidents, according to the Zscaler ThreatLabz report.³⁵

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

This indicates that sophisticated adversaries are specifically targeting Indian digital infrastructure due to its expanded attack surface and the strategic advantage of disrupting India's economic operations.

Analyzing institutional frameworks is essential for evaluating governance structures responsible for data resilience. The 2024 amendment to the Allocation of Business Rules created a National Cybersecurity Secretariat within the National Security Council Secretariat. It tasked the National Cybersecurity Coordinator with coordinating cybersecurity efforts across all departments and ministries.³⁶ This change acknowledges that fragmented sectoral responses are not enough to tackle systemic cyber threats.

The methodology examines how CERT-In, designated as the national agency for responding to cybersecurity incidents, collaborates with the National Critical Information Infrastructure Protection Centre and sector-specific Computer Security Incident Response Teams, such as CSIRT-Fin for financial services and CSIRT-Power for energy infrastructure.³⁷ The effectiveness of these coordination efforts in enabling prompt information sharing, synchronized responses to cross-sector threats, and consistent implementation of security standards across varied organizations is a crucial factor affecting overall data resilience.

The methodology also looks at the intricate relationship between data resilience and economic sovereignty by assessing dependencies on foreign-controlled technology platforms and infrastructure.

Nearly 77 of India's cloud market is dominated by three American companies, while the country's digital ecosystem heavily relies on foreign operating systems, infrastructures, and software. This dependency creates vulnerabilities, as disruptions in foreign-controlled services or restricted access during diplomatic conflicts could hinder Indian economic functions.

The use of digital infrastructure and financial connections as weapons, seen in the SWIFT-based financial exclusion measures against countries like Russia and Iran, shows that reliance on foreign systems creates geopolitical vulnerabilities that can be exploited during conflicts. Thus, the methodology views data resilience not just as a technical cybersecurity issue but as part of strategic autonomy, needing domestic capability development, diversification of technological dependencies, and careful international cooperation to protect sovereignty.

Evaluating the effectiveness of policies looks at government initiatives aimed at improving data resilience against their goals and measurable results. The Digital Personal Data Protection Act 2023, signed into law by India's President and supported by the Draft Digital Personal Data Protection Rules 2025, creates a comprehensive legal framework balancing individual privacy rights with necessary data processing needs.³⁸

The methodology identifies implementation challenges, such as the lack of notified restricted country lists for cross-border data transfers, the pending establishment of the Data Protection

Board, and the requirement for building institutional capacity to enforce the provisions effectively. The Act's connection to the SARAL framework—focused on simplicity, clarity, and contextual definitions—attempts to make compliance straightforward for various stakeholders. However, the actual effectiveness depends on regulatory guidance, consistent enforcement, and stakeholder awareness, which are still evolving.³⁹

The Citizen Financial Cyber Fraud Reporting and Management System, launched in 2021 under the Indian Cybercrime Coordination Centre, provides solid evidence of effective interventions, having saved more than rupees 7,130 crore through over 23.02 lakh complaints by enabling immediate reporting of financial fraud and coordinating with law enforcement and financial institutions to freeze fraudulent transactions.⁴⁰

The Suspect Registry, launched in September 2024, shares suspect identifier data and mule account information with financial institutions. It has blocked transactions worth rupees 8,031.56 crore, preventing fraud before it occurs instead of just responding afterward. These results show that well-planned interventions that combine technology, interagency coordination, and rapid response protocols can have measurable protective effects. However, the 206 percent year-over-year increase in total cyber fraud losses indicates that defensive measures are insufficient to counter rising threats.⁴¹

The methodology recognizes the limitations in assessing data resilience due to the classified nature of certain threat intelligence, incomplete reporting of cybersecurity incidents because organizations are often hesitant to disclose breaches, and the fast-evolving landscape of threats and defenses, which makes point-in-time assessments quickly outdated.

The National Critical Information Infrastructure Protection Centre states that revealing details about breaches in critical infrastructure may not serve national security needs, meaning a full public review of vulnerabilities in the most sensitive systems remains unfeasible.⁴² Additionally, the methodology acknowledges that quantitative metrics like reported incidents or financial losses only reflect aspects of data resilience that can be easily measured, while qualitative factors such as security culture within institutions, effectiveness of threat intelligence sharing, and resilience of backup and recovery systems must be evaluated through indirect indicators.

The need for data resilience ultimately stems from the tension between the opportunities created by India's digital transformation and its inherent vulnerabilities. The Ministry of Electronics and Information Technology's January 2025 report on measuring India's digital economy states that the digital sector now contributes 11.74 percent of national income, with predictions indicating growth to nearly one-fifth of GDP by 2029-30.⁴³

This economic integration means that disruptions to digital infrastructure are no longer just isolated technical failures; they can lead to systemic shocks affecting economic stability, service delivery from the government, and social functions. The methodology used in this report treats data resilience as essential for maintaining India's digital progress, requiring thorough assessment of

threats, capabilities, governance structures, and strategic approaches to ensure that the digital framework supporting India's development remains secure, accessible, and trustworthy against ongoing, sophisticated adversarial threats.



Roundtable Participants

1. Adv. Sujeet Kumar, Hon'ble Member of Parliament, Rajya Sabha, is a member of the Standing Committee on Science Technology, Environment, Forests and Climate Change. He is also a member of the Consultative Committee for the Ministry of External Affairs, GOI, the Indian Council of World Affairs, and the author of the book "AI on Trial."
2. Dr. Rabindra Narayan Behera, Hon'ble Member of Parliament, Lok Sabha, is a member of the Standing Committee of Communication and Information Technology and the Consultative Committee of the Steel Ministry, GOI.
3. Mr. Vinit Goenka is the Secretary of the Centre for Knowledge Sovereignty (CKS) and the author of "Data Sovereignty: The Pursuit of Supremacy."
Member Program Committee, Gandhi Smriti and Darshan, Ministry of Culture, GOI, Former Spokesperson -BJP Delhi Pradesh, Former National Convenor IT Cell BJP, Former Governing Council Member - Centre for Railway Information System (CRIS), Ministry of Railways, GoI, Former Member IT Task Force, Ministry of Road Transport Highways and Shipping, GoI.
4. Mr. Praveen Kumar, IRSE, is the Managing Director of the Dedicated Freight Corridor Corporation of India Ltd, Ministry of Railways, GOI.
5. Dr. C. S. Mohapatra, IES, is the IEPF Chair Professor at NCAER. He is also a former Principal Adviser with the rank of Secretary to the Government of India and a former Additional Secretary in the Ministry of Finance, GOI.
6. Mr. Nitin Khade, IAS, is the Joint Secretary of the Department of Land Resources, Ministry of Rural Development, GOI.
7. Prof. Dr. Unnat P. Pandit serves as the Controller General of Patents, Designs, and Trademarks (CGPDTM), RoC, GI, and SICLDR, GOI.
8. Major General Manjeet Singh, SM, VSM (Retd.), is the Joint Secretary for Cyber at the National Security Council Secretariat (NSCS), PMO, GOI.
9. Mr. Ajay Kumar Yadav, IPS, is the Principal Resident Commissioner of the Government of Himachal Pradesh.
10. Dr. Amit Sharma is the Additional Director General and Advisor for Cyber at the Ministry of Defence, GOI.
11. Mr. Sandeep Bhambure is the Vice President and Managing Director of Veeam India and SAARC.
12. Mr. Agendra Kumar is the Managing Director of Esri India.

13. Mr. Mahesh Jiwade, IRS, is the Private Secretary to the Minister of State for Power and New & Renewable Energy.

14. Mrs. Shubha N. Bhambani, ITS, is the Additional DGT of the Department of Telecommunications, GOI.

15. Mr. Amit Gunvant Bhole, ICAS, is the DyCGA in the Office of CGA at the Department of Expenditure, Ministry of Finance, GOI.

16. Dr. G. Shreekumar Menon, IRS, is the former Director General of the National Academy of Customs, Indirect Taxes, and Narcotics in the Ministry of Finance, GOI.

17. Mr. Satya Narayan Meena, IRSSE, is the Additional CEO and Chief Financial Officer at the Government e-Marketplace (GeM), Ministry of Commerce and Industry, GOI.

18. Mr. Inder Pal Singh Sethi is the former Director General of the National Informatics Centre, GOI.

19. Mr. S. N. Tripathi serves as the Executive Director of the National Thermal Power Corporation.

20. Mr. K. B. Nanda, IAS (Retd.), is the former Financial Commissioner of the Railway Board, former Principal Financial Adviser for Northern Railway and North-Western Railway, former Executive Director at the Ministry of Railways, former Executive Director at Ircon International, and former Director for CCFB Railways in Mozambique, Africa.

21. Mr. Manoj Tandon is the Director of Project Operations and Maintenance at Railtel Corporation of India.

22. Dr. Vijay Rai is the Chief Business Strategist for Governance, Resilience, and Transformation at Veeam Software and a Distinguished Fellow at CKS.

23. Mr. Vijay Kumar is the Senior Vice President and CTO at Esri India.

24. Ms. Sumitra V. Goenka is an Independent Director at Plada Infotech, a Director at Madhyom Communications, and the CEO of Triangleglobal.

25. Mr. Vijay P. Karia is the Chairman and Managing Director of the Ravin Group of Companies.

26. Lt. Gen. Vinod G. Khandare, PVSM, AVSM, SM (Retd.), is the former Principal Advisor at the Ministry of Defence, GOI, former Military Advisor at NSCS, and former Director General of the Defence Intelligence Agency.

27. Lt. Gen. Arun Kumar Sahni, PVSM, UYSM, SM, VSM (Retd.), is the former General Officer Commanding-in-Chief of the Indian Army.

28. Mr. Jayadeva Ranade is the former Additional Secretary at the Cabinet Secretariat.

29. Commodore Naresh Chhabra serves at DACIDS HQIDS, MoD.
30. Brigadier Aman Anand is part of the Indian Army.
31. Col. (Dr.) Anupam Tiwari, Ph.D., is the Advisor for Cyber to the Principal Advisor at MoD in the Indian Army.
32. Col. V. D. Singh (Retd.) was the former Joint Director of IT with DG Info System at Army HQ, a Visiting Faculty at various Institutes, and a Distinguished Fellow at CKS.
33. Col. Pankaj Awasthi (Retd.) is a Cybersecurity Leader.
34. Lt. Col. Nishant Singh (Retd.) is the VP and COO of Gramak Cybertech.
35. Lt. Col. Amitabh Bhardwaj (Retd.) is the Director of Projects at DST, IIT Madras.
36. Lt. Col. Alok Shankar Pandey (Retd.) is the Group General Manager of IT and Chief Information Security Officer at the Dedicated Freight Corridor Corporation of India Limited, GOI.
37. Mr. Pawan Kumar is the Executive Director for Finance and Chief Compliance Officer at Power Finance Corporation Ltd, GOI.
38. Dr. Susil Kumar Meher is the Head of Health IT and CISO at AIIMS.
39. Ms. Arundhati Bhowmick is the Group General Manager and Head of IT at Engineering Projects India Ltd (EPI).
40. Mr. Basudeb Das is the Head of Department for New Technology and Systems and the Chief Vigilance Officer in the Intelligence Department of the Income Tax Department, Ministry of Finance, GOI.
41. Mr. Saurabh Jain is the Deputy Director at Infosource (ITBA), CBDT, GOI.
42. Mr. Harvinder Kumar is the Deputy Director of Income Tax at the Ministry of Finance, GOI.
43. Mr. Yogendra Prasad is the former Advisor at the Department of Telecommunications (DoT), GOI.
44. Dr. Debapriya Dutta is the former Advisor at the Department of Science and Technology, GOI.
45. Mr. Sohan Nautiyal is the Principal Consultant at Digital India Corporation, GOI.
46. Mr. Vipul Srivastava is with the IMC Chamber of Commerce and Industry.
47. Dr. Pankaj Vashist is an Associate Professor at RIS.

48. Mr. Santulan Chaubey is the former Joint Director at the Department of Information Technology for the Government of Delhi.
49. Mr. Digvijaysinh Chudasama is a Partner at Deloitte India.
50. Mr. Ashok Narayanaswamy is a Chartered Accountant and Partner at S. R. Batliboi & Co. LLP.
51. Mr. Amitava Sengupta is the President and Group Chief Digital Officer at RPSG Group.
52. Mr. Eshwar Reddy Keesara is the Managing Director at Dakkhin.
53. Mr. Keshri Kumar Asthana is the Chief Technology Officer for the Public Sector at Microsoft India.
54. Mr. Jeevan Talegaonkar is the Vice President at Jio Platforms Limited.
55. Dr. Ravindra Kumar is the Chief Scientist and Head of ILT at CRRI, GOI.
56. Mr. Mukesh Jain is the CTO and EVP at Capgemini.
57. Mr. Saket Setu is the CEO of Towards Vision Technologies Limited (C-Zentrix).
58. Mr. Rajesh Gupta is the Associate Head of IT for Infrastructure and Security at Perfetti Van Melle.
59. Mr. Golok Kumar Simli is the President of Technology and Innovation (Global) at BLS International. He is also the former Principal Advisor and CTO of Passport Seva Program 2.0 and ePassport, GOI.
60. Mr. Tapendra Dev is the Founder and CEO of Secure Blink.
61. Mr. Kushagra Sharma is the Marketing Head for India and SAARC at Veeam.
62. Mr. Vivek Tiwari is the Founder and CEO of Audix Techno Consulting Solutions Pvt Ltd.
63. Mr. Thirunarayanan Varadadesigan is the Principal Technical Program Manager at Walmart Global Tech, USA, and a member of CKS.
64. Mr. Pratham Vijay Karia is a Director at the Ravin Group.
65. Mr. Viraj Chouhan is the Group Corporate Affairs Officer at RP Sanjiv Goenka Group.
66. Mr. Sanil Namboodiripad is the former Chief Operating Officer at Ingrid Investment Managers Limited.

67. Dr. Anuranjan Misra is a Professor and Dean at Greater Noida Institute of Technology (GNIOT).
68. Mr. Krishan Dev Nidumolu is the Head of Information Security at the Insurance Information Bureau of India.
69. Mr. Manish Chaudhary is the Vice President of Sales at Aathreya Labs Private Limited (ALABS).
70. Ms. Anamika Das is the Head of Advocacy and Strategic Programs at Esri India.
71. Mr. Manoj Gupta is the Senior General Manager at TeamLease Edtech.
72. Ms. Nischala Murthy Kaushik is the CMO at Opus Technologies.
73. Mr. Pulkit Chaudhary is a Data Privacy Expert and Legal Counsel at Sberbank.
74. Dr. Ashish Kumar is a Scientist 'C' at CERT-In, Ministry of Electronics and Information Technology, GOI.
75. Mr. Rishab Gulati is the Editor-in-Chief of NewsX and NewsX World.
76. Mr. Saurabh Sehgal is the Director of Sapphire International School in Greater Noida.
77. Dr. Nagarathana A. is an Associate Professor at the National Law School of India University in Bengaluru.
78. Ms. Ekta Soni is the Assistant Director of Academics and Principal at Sapphire International School.
79. Dr. Kriti Singh is the Honorary Advisor for Media Relations and Research at CKS.
80. Dr. Jinny Tomar is an Advocate at the Delhi High Court and with SCS Partners.
81. Ms. Anusha Soni is the former Editor of CNN News 18.
82. Mr. Naresh Kumar is the AGM at BSNL.
83. Dr. Satbir Yadav is the former DGM at CSD, Ministry of Defence, GOI.
84. Mr. Swapan Biswas is a Consultant for CSC e-Governance Services with the Government of India.
85. Mr. Yuvraj Chopra is the Country Advocacy Lead for Agri Solutions at BASF India Ltd.

86. Mr. Kawal Walia is the EVP at WalSof Technologies.

87. Wing Commander Deepak Prasad is with the Indian Air Force.

88. Mr. Sanjay Sharan, IRS, is the former Commissioner of Customs and CGST, GOI.



Findings

This section summarizes discussions from three roundtables organized by the Centre for Knowledge Sovereignty (CKS) on data governance, cybersecurity, and resilience in India. These roundtables brought together senior government officials, military leaders, cybersecurity experts, infrastructure managers, technology executives, and policy specialists to explore the challenges and opportunities in India's digital ecosystem. The discussions addressed critical infrastructure vulnerabilities, regulatory frameworks, emerging AI threats, and the goals set in Vision 2047.

The Evolution of Digital Colonization

Human conflict has progressed through three distinct stages over millions of years.⁴⁴ The first stage, lasting over 2.3 million years, involved military colonization through the use of physical force, including stone tools, swords, and cannons. The second stage emerged about 200 years ago with the advent of energy colonization, in which nations controlled oil resources without armed conflict. The third and most concerning form is data colonization, which began 40-45 years ago, representing a new way to control and influence that operates invisibly yet powerfully.

Data colonization signifies a significant shift in global power dynamics. Unlike earlier forms of colonization that needed a physical presence or control over tangible resources, data colonization functions through digital infrastructure, algorithms, and information flows.⁴⁵ This type of control can sway elections, manipulate markets, extract economic value, and threaten national security without violence.

India's Current Threat Landscape

Geopolitical Dimensions

India is facing a complex and growing threat environment marked by more frequent attacks, increasing technical sophistication, and various methods targeting critical infrastructure, financial systems, personal data, and government operations. The geopolitical context heightens these concerns.

China's Critical Infrastructure Attacks

October 2020 Mumbai power outage shows how critical infrastructure has become a key area in today's geopolitical competition. The disruption stopped trains and shut down stock exchanges and hospitals for hours.⁴⁶ This incident highlighted the vulnerabilities of interconnected urban systems. Its importance lies not just in how it was executed but also in when it happened and its strategic purpose.

The cyber-attack took place during a crisis on the Sino-Indian boundary. Malware was introduced into Maharashtra's electricity grid while military tensions in Ladakh were high. Investigations

found that RedEcho, a Chinese state-sponsored group, targeted nearly a dozen critical points in Indian power infrastructure.⁴⁷ This was a deliberate strategy by China in response to India's military positioning along the Line of Actual Control and its economic actions against Chinese interests.

This incident highlighted a major vulnerability: India's reliance on Chinese hardware in its power infrastructure created opportunities for attacks. The malware's persistence indicated it was set up in advance for future actions rather than immediate harm, signaling China's capability to exert pressure. India's creation of CSIRT-Power in April 2023 and its security audits of 30 state dispatch centers by March 2024 demonstrate an awareness that securing critical infrastructure in the digital realm is now crucial to national security amid great-power competition.⁴⁸

China employs about 20,000 personnel to specifically target India's digital infrastructure. Their methods go beyond traditional attacks on government systems to include hospitals. These sophisticated tactics extract personal data on targeted individuals, including political leaders and senior officials. This focused approach highlights the strategic nature of modern cyber warfare, where gathering intelligence and creating leverage are primary goals.

The ongoing confrontation that began in May 2025, known as Operation Sindoor, and the evolving international relations, showcase significant AI and data elements. During Operation Sindoor, state actors displayed aggressive cyber capabilities, hitting government websites with 80-90 million requests per second at peak times. Thanks to coordinated efforts from government cybersecurity agencies, including red teams and AI-driven threat detection systems, no major incidents occurred during this critical time.

Tariff dynamics with major powers are likely to enhance international interest in understanding India's strategic planning and leadership viewpoints. The Nayara Energy incident, in which a Western company cut off an Indian company's cloud access due to geopolitical tensions, highlights data weaponization and sovereignty infringement. This incident exposed India's vulnerability regarding strategic dependence for the first time, showing how foreign control of important digital infrastructure can be used as a geopolitical tool.

The evolving threat landscape also includes the development of BioWare utilizing AI to assess racial characteristics and predict behaviors during crises. This approach requires access to Indian demographic and health data, making data protection crucial not just for domestic needs but also for national security.

In response to these revelations, the central government established Computer Security Incident Response Team Power (CSIRT-Power) in April 2023 exclusively for the power sector, alongside Security Operation Centres at GRID-INDIA and POWERGRID for continuous monitoring of critical assets. By March 2024, 30 out of 35 State Load Despatch Centres had conducted Vulnerability Assessment and Penetration Testing cyber security audits, representing significant progress in defensive preparedness. These measures underscore the imperative for continuous

cyber vigilance, infrastructure modernization, and the development of offensive cyber capabilities to establish credible deterrence against state-sponsored cyber operations targeting critical national infrastructure.

The Ransomware Epidemic

According to the Indian Computer Emergency Response Team's India Ransomware Report 2024, ransomware has become the primary cyber threat for Indian organizations.⁴⁹ In 2024, LockBit, RansomHub, and KillSec emerged as leading ransomware groups impacting India. LockBit remained the most active, especially since its leaked source code allowed new players to enter the attack scene.⁵⁰

The manufacturing sector experienced the highest number of ransomware attacks in 2024, followed by the finance and information technology sectors. This pattern indicates that attackers focus on industries in which disruptions exert the greatest pressure to pay ransoms. A troubling trend is the increased targeting of virtualized environments in data centers, particularly VMware ESXi hypervisors, enabling ransomware actors to encrypt multiple virtual machines at once.⁵¹

Ransomware operators are shifting toward more complex extortion tactics beyond traditional file encryption.⁵² Double extortion involves encrypting data while also stealing copies, then threatening to publish the stolen information if ransoms are not paid, making backup recovery ineffective. Triple extortion goes further by using stolen data to target customers or business partners with denial-of-service attacks, increasing pressure on victim organizations.⁵³

The hacktivist group KillSec has shifted to ransomware by exploiting weak configurations in public cloud storage and access management policies.⁵⁴ Rather than sending ransom notes, they list stolen data on leak sites for sale.⁵⁵ Their customized extortion methods show increasing psychological sophistication—attackers now directly contact senior executives and IT administrators, applying personal pressure with threats of follow-up attacks, data exposure, and disclosures to clients and regulators.⁵⁶

When ransom demands are ignored, some attackers escalate their tactics by emailing regulatory authorities and alleging compliance failures related to data protection.⁵⁷ Fake ransomware campaigns add complexity, as groups use previously stolen data or create fake datasets to claim attacks and extract payments even without a real breach.

Major Data Breaches

Significant data breaches affecting millions of Indian citizens have exposed serious weaknesses in both public and private digital infrastructures. In July 2024, Bharat Sanchar Nigam Limited (BSNL), one of India's largest state-owned telecom firms, suffered a breach impacting sensitive data, including International Mobile Subscriber Identity numbers, SIM card information, server snapshots, and extensive customer data.⁵⁸ This data subsequently appeared for sale on dark web marketplaces, revealing critical vulnerabilities in BSNL's cybersecurity framework and raising concerns about misuse through SIM swapping and targeted phishing.⁵⁹

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

The financial services sector experienced particularly damaging breaches. Angel One had private information from eight million customers leaked. Cryptocurrency exchange WazirX was breached, resulting in the loss of \$230 million in assets due to vulnerabilities in its multi-signature wallet system.⁶⁰ Star Health Insurance faced a breach affecting 31 million customers, with stolen data, including medical records and policy information, sold on the dark web for up to \$150,000.⁶¹ Hathway Cable & Datacom Ltd experienced a breach that exposed personal data of over 41.5 million customers, with attackers leaking 12 GB of sensitive information.⁶²

Government digital services have also shown weaknesses. The eMigrate Portal, established by the Ministry of External Affairs to assist Indian laborers moving abroad, reported a breach that affected around 200,000 users.⁶³ Compromised data included full names, email addresses, phone numbers, dates of birth, mailing addresses, and passport information, which were posted on cybercrime forums.⁶⁴ The Telangana Police Hawk Eye mobile app, designed for citizens to report crimes, suffered a breach impacting about 200,000 users, due to vulnerabilities in its backend system.⁶⁵

State-Sponsored Threats and Advanced Persistent Threats

State-sponsored actors and advanced threat groups are increasingly targeting India's government and critical infrastructure using advanced techniques characterized by careful reconnaissance, custom malware, and long-term infiltration goals. The FlightNight cyber espionage campaign specifically targets Indian government and energy sectors, employing modified HackBrowserData tools to steal sensitive information through Slack channels and phishing emails disguised as official invitations.⁶⁶

LightSpy represents sophisticated spyware aimed at iOS devices, showing that attackers can compromise mobile platforms that users often consider secure.⁶⁷ The blending of hacktivism and ransomware operations indicates that geopolitical and ideological conflicts are transforming cyber threats, resulting in hybrid groups that mix activism, state-sponsored actions, and profit-driven crime.⁶⁸

Cyber attacks on the Indian government surged by 138 percent from 2019 to 2023.⁶⁹ This increase results from both improved detection capabilities and a genuine rise in threats motivated by intelligence collection, economic espionage, and potential preparations for future conflicts.⁷⁰ Telecommunications networks proved particularly vulnerable, as shown by the BSNL breach and global incidents like the Salt Typhoon operation that targeted telecom infrastructure. This situation calls for enhanced supply chain monitoring and procurement from reliable vendors.

AI-Enhanced Attacks and Social Engineering

Phishing campaigns against Indian users rose by 175 percent in June 2024 compared to the previous year, with 82.6 percent using AI-generated content to appear more convincing by mimicking trusted sources.⁷¹ Artificial intelligence is making phishing attacks more sophisticated by generating emails that closely resemble the tone, style, and branding of legitimate entities.

Cryptocurrency and Blockchain Threats

The expanding cryptocurrency ecosystem in India faces unique threats that mix traditional cybersecurity vulnerabilities with blockchain-specific attack methods. The WazirX breach, which resulted in \$230 million in stolen assets, involved the theft of over 200 crypto assets, including \$96.7 million in Shiba Inu tokens, \$52 million in Ethereum, \$11 million in Polygon, and \$7.6 million in Pepe.⁷² This incident highlights both the potential value at risk and the technical expertise needed to compromise multi-signature wallet systems.

Cryptojacking operations saw an increase of 409 percent, as attackers target computational resources for unauthorized cryptocurrency mining instead of directly stealing digital assets.⁷³ The convergence of ransomware operations with cryptocurrency payment mechanisms creates challenges for law enforcement, as blockchain transactions provide partial anonymity complicating fund recovery and perpetrator identification.

The Imperative of Data Sovereignty

Data sovereignty has become crucial for economic growth and national security. Environmental and economic security are tightly linked through data infrastructure and control. India needs to own and manage its data rather than relying on foreign platforms and infrastructure. The United States' dominance in big data analytics emphasizes the competitive nature of data sovereignty globally.

Data sovereignty relies on key principles. First, data integrity must be ensured through strong verification and validation systems that guarantee accuracy and reliability. Second, data security needs thorough protection against cyber threats, which are at the forefront of future conflict. The view that "the Third World War will be in the cyber world" reinforces this acknowledgment. Third, data resilience involves building systems that are robust, flexible, and easy to recover, ensuring data remains accessible even during disruptions or attacks.

India should develop homegrown data ecosystems with support from both government and military institutions. This civil-military framework recognizes that data infrastructure serves both commercial and defense needs.

The establishment of Indian data centers within the country's borders is crucial for maintaining sovereignty. Policies must enforce local data storage, backup processing within Indian jurisdiction, and the development of national databases.

The Centre for Knowledge Sovereignty, founded in 2011, has been at the forefront of advocating for data sovereignty in India. The organization introduced the term "data sovereignty" when it was not well-known in the country. At that time, many people doubted the need for data centers on Indian soil since overseas hosting services were cheaper. There was widespread skepticism, with many viewing data infrastructure in India as unrealistic.

The think tank's influential work led to the publication of "Data Sovereignty: The Pursuit of Supremacy" in 2019. Written by former Directors General of Military Operations, defense intelligence officials, and technology experts, this book has become required reading in military circles, the Parliament library, IIMs, IITs, and various esteemed institutions across the country, with over 40,000 copies distributed.

AI Capabilities

Without enough control over data and AI capabilities, India risks economic exploitation by other nations. This exploitation can manifest in various ways, from stealing intellectual property to market manipulation supported by advanced data analysis. The characterization of future warfare as largely cyber-based reinforces the importance of data infrastructure for national defense.

India's transportation infrastructure faces significant cybersecurity challenges. The Dedicated Freight Corridor Corporation of India Limited (DFCCIL) manages two major corridors: the Eastern Corridor covering 1,300 route kilometers from Ludhiana to Sonagar and the Western Corridor from Dadri to JNPT.⁷⁴ The entire system relies on digital data, with operation control centers supervising train operations.

These systems are highly susceptible to cyber-attacks, which could manipulate turnout and point systems, potentially rerouting trains and causing severe accidents. Multiple layers of protection have been implemented, including disaster management centers that allow train operations to continue even if primary systems fail.

AI is utilized in machine vision inspection systems to automatically identify defects in rolling stock, alerting control centers to prevent derailments. Drone-based inspection systems using AI also monitor infrastructure. However, the digital nature of these systems introduces new vulnerabilities, as every train movement depends on data processing and communication.

The railway sector has additional vulnerabilities. If adversaries sold duplicate tickets, many passengers could hold reservations for the same seat at the same time, creating chaos and requiring more security personnel than are available. Such coordinated attacks at multiple stations could be perceived as acts of war without conventional weapons.

India's railway ticketing system undergoes 400-600 hacking attempts daily. The exposure of this system—where tickets are sold to multiple individuals simultaneously due to security failures—highlights the real consequences of weak cybersecurity. Systems managing 400,000 to 600,000 transactions daily illustrate the scale of infrastructure needed to support India's large population and economic activity.

India's 6.62 million kilometers of roads are being digitalized, along with the management of over 300 million vehicles, which creates significant challenges in traffic management. Each morning, journey planning begins with mobile apps that quickly convey data to servers. Users download

many apps without reading data protection terms, often accepting consent without understanding the implications.

Daily planning with various transaction apps means data sharing occurs everywhere without clarity on how it is handled or protected. Millions of trips generate daily data, but no comprehensive domestic system exists. Without local technology, risks and vulnerabilities remain. All 6.62 million kilometers of roads are geotagged, raising fears that adversaries could pinpoint exact locations. In wartime, knowing the precise site of bridges or tunnels can make strategic targeting easier without conventional combat.

International data-sharing policies should not provide exact locations to foreign servers, especially for critical infrastructure. Regular audits of apps, implementation of multi-layer security systems, and ensuring effective execution of the Digital Personal Data Protection (DPDP) Act require serious attention. Asset inventories should track whether software is open-source or properly licensed, as many systems include expired or unlicensed software, creating risks for data leaks and unauthorized access.

AIIMS attack

Healthcare records have become more vulnerable globally than financial records, yet organizations lack cybersecurity maturity models to guide their efforts. A massive ransomware attack on AIIMS on September 22, 2022, at 7:30 AM triggered a national alert, prompting responses from the PMO, defense ministry, and other government agencies. The organization avoided data loss because its backup systems completed their cycle right before the attack.

Recovery took 15 days because it took time to identify which infrastructure components were infected, given inadequate preparation. Attackers usually know the infrastructure better than defenders, understanding frameworks and vulnerabilities. This requires changes to entire 2022 frameworks and policies during recovery, highlighting the importance of proactive measures over reactive responses.

AIIMS operates over 17,000 PCs on a vast 100-gigabyte network serving 100 organizations, presenting enormous restoration challenges without adequate forensic planning. Data classification is key since healthcare records often require different protection levels compared to financial data. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) must be clearly defined, with both disaster recovery and backup recovery solutions in place.

Narcotics proliferation

The narcotics industry is the world's second-largest sector after arms manufacturing. Drug trafficking networks use highly sophisticated data mining techniques. Traffickers in places like Dubai, Pakistan, Afghanistan, Iran, and Myanmar know exactly which drugs to send to various parts of India based on seizure data and consumption patterns. This precision shows how criminals exploit data vulnerabilities.

Current practices of quickly making drug seizures public, including operational details and personnel involved, compromise security and allow traffickers to adjust their tactics. A Drug Seizure Data Protection Regulation Act is needed to balance transparency with security in operations.

Digital payments system

The development of India's digital payment system reflects both progress and vulnerability. After demonetization on November 8, 2016, India's UPI transactions increased from 91 crore annually in 2017 to 20 billion transactions worth ₹24.85 lakh crores recently. Each transaction metro travel, FASTag use, NEFT, RTGS—is monitored on dashboards, representing critical infrastructure that cannot afford to fail without stopping the economy.

To achieve the \$5 trillion economy goal, strong digital infrastructure is necessary. Current trends suggest reaching this target by 2027, with potential for a \$30 trillion economy by 2047. The Digital Public Infrastructure (DPI) concepts developed during G20 showcase India's capacity for both domestic and international needs.

However, vulnerabilities persist even in high-priority systems like NPCI and financial transactions. The data from personal banking shows weaknesses—a simple credit inquiry for a loan can result in days of calls from banks nationwide, all possessing complete personal information, including date of birth, PAN card number, Aadhaar number, and employment details. This illustrates that assumptions about data safety based solely on its location within the country do not match reality.

Establishing a national consent management system to implement the DPDP Act could help address these issues. Without unified systems, every ministry and department may create different consent processes, resulting in fragmented and vulnerable systems.

A critical vulnerability exists: attacking data centers does not require direct access to servers. Simply targeting power supplies through weak Operational Technology (OT) systems can produce similar outcomes. The average age of infrastructure in the power sector or oil and gas is around 30-40 years, while IT technology refreshes every 3-5 years. OT systems are updated every 20-40 years, leading to major vulnerabilities.

Manufacturing companies are disproportionately impacted by ransomware attacks each year. Major brands experience frequent malware attacks. Even with IT-OT convergence, there is no standard framework for securely integrating these systems. Organizations undertake implementations without guidance, leaving critical infrastructure exposed.

Data discovery efforts often find that most organizations lack awareness of their data landscape. Data classification and visibility are essential for effective protection. Business Impact Analysis (BIA) helps pinpoint crucial infrastructure and apply suitable controls, followed by Business Continuity Planning (BCP) for resilience. These fundamental steps frequently receive inadequate attention.

Energy resilience is vital for all digital operations. If energy infrastructure fails, discussions about resilience, recovery, and protection become pointless. Society depends so greatly on digital systems that younger generations haven't learned paper-based practices. Defense forces continue to emphasize these skills—The Corps of Signals still teaches Morse code so personnel can survive and communicate if complex systems collapse.

DPDP Act as an enabler

The DPDP Act was enacted in 2023, but rules are still being crafted, creating uncertainty for organizations trying to comply. The main principle links data sovereignty to jurisdiction: if citizens create data, that data should belong to the country. This idea of data ownership was insufficiently addressed in recent international frameworks like the UN Convention on Cyber Crime, which focused more on criminality than on ownership and sovereignty.

The significance of data-oriented jurisdiction is immense. Data owners cannot control where or how their data is used, and the importance of data ownership should be recognized. However, this critical concept is often absent from broader policy discussions. Recent UN General Assembly sessions failed to adequately address transnational infrastructure ownership and accountability.

There is strong support for expediting the Digital India Bill since the Information Technology Act of 2000 is outdated. Twenty-five years is far too long in the digital realm, where even 25 days can feel excessive. The absence of comprehensive legislation puts India at a disadvantage, with inadequate legal frameworks and judicial precedents for addressing AI-related matters.

Operationalizing the DPDP Act remains incomplete even after its passage. A key requirement is an independent data protection board that must have real autonomy, not just nominal independence. Various regulatory frameworks, including RBI, SEBI, and NDHM, must align to prevent the creation of disparate pillars that pull in different directions.

India should establish privacy-preserving data trusts across sectors while building data protection skills. Balancing sovereignty amid geopolitical challenges requires India to publish restricted country lists that remain undisclosed, hindering cross-border data transfers, especially for small businesses and startups trying to operate internationally.

Deepfakes

The Bharatiya Nyaya Sanhita 2023 (BNS) made the dissemination of misinformation and disinformation, including the creation and distribution of deepfake content, illegal.⁷⁵ Given deepfakes' potential to distort reality and cause harm, BNS provides essential tools to penalize those who misuse AI technologies. This legal framework safeguards informational integrity and public trust.

To turn legal and regulatory requirements into actionable steps, India has set up institutional mechanisms, including Grievance Appellate Committees that provide forums for users contesting

intermediary decisions and the Indian Cyber Crime Coordination Center (I4C) coordinating responses to cyber-crime across states.⁷⁶

However, gaps in implementation persist. Even with various regulatory bodies (CERT-IN, NPCI, CEI Standards, MEITY Standards), none integrate into a shared body of knowledge giving CISOs strategic and operational direction. Without coherent frameworks, each organization creates its own security measures, missing opportunities for collective progress.

Organizations face rapidly evolving technologies and regulations. Free tools lure users to install them and accept all terms without reading, which can lead to possible data exposure. Organizations that have been around for decades have accumulated large data reserves but struggle to grasp the DPDP Act's implications amid constantly changing regulations, including the Digital Data Act and new AI legislation.

The need for a unified compliance dashboard that interprets requirements across multiple acts remains unmet. Current methods require each organization to decipher requirements independently without guidance. Sector-specific challenges complicate matters—some operations involve critical infrastructure needing strong protection, while others handle less sensitive tasks. Applying the same standards across all situations results in unnecessary costs and efforts.

International Framework Comparisons

The EU's GDPR often serves as a reference point, but India needs approaches that fit its context instead of simply copying European or American models.⁷⁷ The foundational concepts come from the US Patriot Act, particularly sections related to data from specific jurisdictions. This law led to the Cloud Act and influenced the important case between Spain and Google that shaped the EU GDPR framework.

Europe's self-sovereign identity framework, based on blockchain services, offers significant opportunities. While Western nations struggle with this technology, India could advance by implementing a strong blockchain-based identity management system that supports the DPDP Act. This could give India an edge over developed countries facing similar challenges.

The idea of data embassies—where data from a country is stored in another country but follows the laws of its home nation—raises interest because it could improve resilience by distributing data geographically while maintaining legal sovereignty. This method requires careful consideration about which countries are trustworthy and how to guarantee real control instead of just nominal control.

India's unified data approach in sectors like insurance provides advantages over the fragmented American systems where companies maintain separate databases. By utilizing this structural benefit and tackling security gaps, India could emerge as a leader in secure data management rather than merely following existing frameworks.

Data Resilience and Business Continuity

Beyond Security to Resilience

Although organizations spend a lot on security measures, their ability to recover from incidents is vital. Data resilience means creating systems that can withstand, adapt, and recover quickly. Data mobility, or portability, allows for data recovery anywhere if the primary infrastructure is compromised or controlled by attackers.

Research shows that globally, 2,000 companies lose \$400 billion each year, averaging \$200 million lost per company per outage. Data downtime results in reputational damage and operational disruption that can threaten an organization's survival. For India, as it aims to become a \$5 trillion economy, data unavailability halts business activity—cutting off the oxygen supply for economic operations.

Organizations face a perfect storm of complexity and threats. Many companies fail not due to insufficient funding or policies but because of a lack of preparation and readiness. Misjudging preparedness carries risks that border on recklessness. Digital transformation, essential for Viksit Bharat, cannot proceed without addressing resilience fundamentals.

Research with major consulting firms indicates that while 30 percent of CIOs believe their organizations have above-average data resilience, actual evaluations find only 10 percent genuinely achieve this level. This troubling gap between perception and reality leaves most organizations in a vulnerable position. Resilience is not just about managing risk; it's about survival.

Metrics and Standards

The absence of resilience standards in India persists despite the critical need for data interoperability, which fundamentally relies on these standards. Without them, the economic opportunities associated with data and data resilience cannot be fully unlocked. Tiered assessments and metrics are essential, particularly those focusing on Mean Time to Detect (MTD)—globally advised to be under one hour—and Mean Time to Return (MTR)—recommended to be under 72 hours.

These metrics provide clear targets instead of vague goals. Organizations can measure performance, identify weaknesses, and monitor improvements over time. Without measurements, claims about resilience or security remain unverified and subjective. Developing and adopting Indian resilience standards would enable consistent evaluations across sectors and organizations.

In 2024, India saw 369.01 million malware detections across 8.44 million endpoints, averaging 702 detections per minute.⁷⁸ This is an improvement from 2023's 400 million detections across 8.5 million endpoints.⁷⁹ India achieved Tier 1 status in the Global Cyber Security Index released by the International Telecommunication Union, scoring 98.49 and ranking among 47 leading nations that show a strong commitment to cybersecurity practices.⁸⁰

However, new threats, especially those driven by AI, challenge this progress. Adaptive malware, AI-generated phishing attempts, and data-focused ransomware reveal how quickly attackers exploit technological advancements. The 26 percent drop in cybersecurity incidents and Tier 1 GCI ranking show improvements in policy and technical capability.⁸¹ However, sophisticated adversaries continue to evolve their methods.

Business Continuity Planning : From backup to guaranteed recovery

Backup alone is not enough as backup alone does not ensure continuity. Modern attacks increasingly target backup repositories, identity systems, and recovery infrastructure itself. True data resilience requires the **assured ability to recover clean, trusted data at speed**, even when primary environments, credentials, or management planes are compromised.

Organizations must move beyond treating backup as a compliance checkbox and instead adopt **recovery-first design principles**, where restoration speed, integrity validation, and operational continuity are engineered outcomes rather than best-effort responses. Data classification remains essential, but classification must directly inform **recovery prioritization**, ensuring that mission-critical systems are restored first with verified data integrity.

Organizations must quickly identify compromised infrastructure and effectively restore operations. Data classification is crucial—different data types need various levels of protection. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) must be clearly defined, with data encrypted and both disaster recovery and backup recovery solutions in place.⁸² Clear Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) must be supported by **immutable backup architectures**, isolated recovery environments, and regular recovery validation exercises. Disaster recovery and backup recovery should not be treated as separate disciplines; instead, they must operate as **integrated resilience capabilities** that can restore services across on-premises, cloud, and hybrid environments.

To support consistent execution, organizations should adopt **cyber resilience maturity models viz model created from inputs of various companies and organizations (namely SMEs/ Expert) and the most prevalent been used is “Data Resilience & Maturity Model by Veeam”** (DRMM) that translate policy intent into operational readiness. These models should guide CISOs and infrastructure leaders in aligning people, process, and technology—recognizing that automation and orchestration are essential force multipliers in environments facing persistent skills shortages.

A comprehensive national data resilience strategy should be built on five pillars: Policy (integrating resilience into cyber crisis management), Predict and Protect (ensuring supply chain security), Prediction capability (developing indigenous and multi-source threat intelligence along with incident response), Partnership (forming public-private partnerships for critical infrastructure), and Privacy (ensuring proper rules for implementing the DPDP Act).

Cyber Resilience Maturity Model (Indicative)

This table illustrates the progressive stages through which organizations evolve from basic data protection to assured data resilience. Higher maturity reflects improved recoverability, operational continuity, and confidence under disruption.

Dimension	Initial / Ad-hoc	Defined	Managed	Optimized
Strategy & Governance	Data protection treated as an IT task; resilience not linked to business outcomes	Basic continuity objectives defined (RTO/RPO documented but inconsistently applied)	Resilience aligned to business priorities; recovery objectives governed and reviewed	Resilience treated as a strategic capability with board-level visibility and accountability
Data Protection Approach	Backups exist but coverage, consistency, and integrity are uncertain	Standardized backup policies in place across major systems	Protection policies tiered by application criticality and data sensitivity	Protection designed for assured recovery, with immutability and isolation as defaults
Recoverability & Continuity	Recovery success depends on manual effort and individual expertise	Recovery procedures documented but rarely tested end-to-end	Regular recovery testing validates RTO/RPO and application dependencies	Continuous verification of recoverability with predictable, repeatable outcomes
Recovery Speed & Confidence	Restoration is slow, error-prone, and uncertain	Recovery timelines estimated but not consistently achieved	Recovery performance measured and tracked against defined targets	Rapid, trusted recovery with minimal data loss and high confidence
Technology & Architecture	Fragmented tools and siloed environments	Standard platforms adopted for backup and recovery	Integrated architectures support hybrid and multi-environment	Architected for portability, reversibility, and clean recovery

Dimension	Initial / Ad-hoc	Defined	Managed	Optimized
			recovery	across environments
Operational Readiness	Incident response is reactive and uncoordinated	Roles and responsibilities defined but inconsistently executed	Coordinated recovery workflows supported by automation	Orchestrated recovery with minimal manual intervention
People & Skills Dependency	Heavy reliance on individual “heroes”	Core skills concentrated in small teams	Skills augmented by automation and guided processes	Systems designed to reduce cognitive load and skills dependency
Testing & Validation	Testing is rare or event-driven	Periodic testing of selected systems	Regular, scenario-based recovery exercises	Continuous validation embedded into operations
Measurement & Metrics	No objective resilience metrics	Basic tracking of backup success	Defined metrics for recovery time and data loss	Resilience measured through recovery assurance, speed, and confidence
Overall Outcome	Data may exist but recovery is uncertain	Recovery possible but disruptive	Recovery reliable for most critical systems	Data resilience assured even under severe disruption

Technology Dependencies and Indigenous Capabilities

The Indigenous Technology Gap

Discussions consistently highlighted the need for developing indigenous technology to ensure true data sovereignty. Concerns exist regarding whether India has its own operating systems, domain name systems, or fully home-grown geographic information systems. The absence of these

foundational technologies creates dependencies that adversaries could exploit during conflicts or diplomatic tensions.

India's geospatial infrastructure implementation across sectors—from urban planning to agriculture—often lacks sufficient cybersecurity measures. While financial sectors like NPCI prioritize protection, non-financial infrastructures such as power grids, telecom networks, and city management systems receive less attention. The decentralized nature means each department manages its own IT and cybersecurity frameworks, creating expertise gaps among thousands of organizations that handle digital infrastructure.

In many large global geospatial initiatives, data protection and cybersecurity receive minimal focus, often treated as afterthoughts with very little funding allocated. Mid-sized and smaller programs often overlook these issues entirely, even as awareness grows. The challenge extends beyond awareness; it requires building the right skills at every departmental level, especially in decentralized infrastructure ownership.

The push for locally made solutions gained traction after Operation Sindoor and recent global events. However, implementation has been slow until recent developments increased awareness. True sovereignty demands adherence to local laws. Large companies claiming to host data in India must ensure that operational control remains in India rather than overseas.

Cloud and Software Dependencies

The rise of cloud-first and Software-as-a-Service (SaaS) strategies over the past 2-3 years has introduced new vulnerabilities.⁸³ Even insisting on India-based hosting for critical infrastructure does not guarantee control, as software accessing data may operate from outside the country. The threat of foreign governments making arbitrary decisions that affect Indian data access is very real.

Simple systems, such as individual aircraft, can be remotely disabled by manufacturers, and authorized dealers can deactivate cars brought in for service. Solar panel inverters generate significant analytical data about panel performance and electricity generation patterns. AI systems have returned specific company data that was never explicitly uploaded, likely obtained from phones or servers.

Organizations tend to focus on cybersecurity compliance rather than real implementation, often opting for paper protections over actual safeguards. They may meet various requirements but lack the true capability to fend off attacks because proper policies are missing, even if documentation suggests otherwise. The challenge lies in moving beyond compliance checklists to adopting proactive measures that effectively protect critical infrastructure.

Digital Infrastructure Development

Direct data feeds into online systems show that real-time data integration capabilities are either under development or in the planning stages. Design considerations for data architecture emphasize systems that support efficient data analysis while ensuring security and integrity.

Railway infrastructure systems that handle hundreds of thousands of transactions daily demonstrate the scale needed to support India's large population and economic activity.

Big data analytics capabilities are key areas where India needs a competitive advantage. Comparisons with global leaders suggest the goal should be to match capabilities while building local capacity. The focus on analysis that can "integrate all" reflects ambitions for comprehensive data platforms that gather information from various domains and sources.

However, submarine cables and terrestrial communication networks are critical vulnerabilities. These infrastructure elements are generally owned by companies, creating accountability gaps since these companies respond to shareholders and boards, not nations or citizens. When cables fail or are taken down, questions arise about accountability and who can compel repairs or guarantee standards. These issues lack clear resolutions, leaving dangerous ambiguities.

The Human Factor and Capacity Building

Skills Shortage and Training Needs

Traditional approaches of "people, process, technology" have changed—technology now shapes both processes and people. This technological influence fosters a mindset of increasing reliance on systems that people don't fully understand. Between protection and resilience lies the need for vigilance, which involves constantly monitoring trends and emerging threats.

The skills shortage poses a significant challenge, with India lacking over two million cybersecurity professionals. Major consulting firms are hiring around 100 new employees each week to meet the growing demand. Without enough skilled personnel, even the best policies and technologies cannot offer strong defense.

Assessment suggests that personnel importance is at 40 percent, processes at 40 percent, and technology at 20 percent. A phishing simulation revealed that 77 percent of employees clicked on malicious links, and nearly 50 percent entered credentials. This demonstrated that without sufficient awareness, even advanced technology cannot guarantee resilience or data protection.

Talent forms India's human firewall. The shortage of roughly five lakh cybersecurity professionals creates an urgent need to build a solid base of experts combining technical depth with strategic thinking. Four key skills are essential: cyber risk intelligence, AI-augmented security management, data privacy expertise, and human-centric security design.

Educational Initiatives

complete course materials online with flexible examination opportunities at no cost. Students who pass the examinations visit ISRO facilities, including satellite control centers, where they interact with scientists and engineers.

These initiatives aim to develop future generations of professionals who view cybersecurity not as abstract concepts but as essential parts of national operations. The combination of education and

exposure to critical infrastructure gives youth the chance to understand the complexity and significance of national systems.

Creating fellowships to produce "a million cyber karma yogis"—a workforce dedicated to cybersecurity as both a career and a mission—represents one approach. Research and development must work in tandem with action instead of remaining isolated. Threat detection research, AI-driven predictive modeling, incident response studies, zero-trust infrastructure research, quantum-resistant cryptography, privacy-preserving computing, and sovereignty frameworks all need continuous investment.

Awareness and Cultural Change

Education about the significance of personal data should start in schools rather than waiting until individuals are older. Awareness developed at a young age persists throughout lives and careers. Fintech conference executives readily shared personal details and subscribed to platforms to win small prizes, despite understanding cybersecurity risks. Even educated professionals often underestimate the value of data, showing that awareness does not always translate into appropriate behavior.

Ongoing training programs need to replace outdated methods, with independent organizations offering certifications similar to those provided by professional medical organizations like the Medical Council of India. However, awareness alone is not enough; implementing certified programs requires CISOs and security managers to hold professional certifications and establishing thorough Governance, Risk, and Compliance (GRC) frameworks for ongoing monitoring.

Several urgent areas need focus: eliminating tick-box compliance strategies, redefining procurement processes to go beyond selecting the lowest bidder for security solutions, implementing certified programs, and establishing comprehensive GRC frameworks. These systemic changes require an institutional commitment that extends beyond individual awareness.

Emerging Technologies: Opportunities and Threats

Artificial Intelligence

The growth of artificial intelligence brings both opportunities and challenges. An analysis from 2014 showed that every email, message, and social media post goes through servers that analyze mindsets to influence them.⁸⁴ This technology, created well before AI became common, means external forces could potentially sway elections and voting patterns in India.

The "DILEMMA" framework for understanding data challenges includes digitization and data consolidation, intelligent extraction, local recovery abilities, actionable data extraction, master data management, meaningful insights, and usable data in the AI era. This framework needs to align with our understanding of workload (the business), workforce (who handles data), workspace (where data is managed—on-premise, cloud, hybrid), workflow (how applications access data), and web (managing online exposure).

The movement of data and workspaces creates operations without borders in the AI era. The government cannot build essential capabilities alone; partnerships with the industry are vital. Developing use cases for AI's impact on key areas like health, education, transportation, and agriculture is still in early stages. India must create AI models the "India way," with explanation features and human oversight instead of mimicking other countries.

AI-generated content makes phishing campaigns more effective by mimicking trusted entities convincingly. AI-driven chatbot scams lure victims into authentic conversations to gather personal information. Large language models enable cybercriminals to craft convincing phishing emails and malware without requiring advanced technical skills.

Quantum Computing Threats

Many experts worry that quantum computing could compromise current encryption standards. Ensuring quantum-safe encryption has not been a major topic in Indian discussions, while neighboring countries are advancing rapidly. If adversaries achieve quantum computing breakthroughs first, all existing encryption could be compromised at once, leading to disastrous outcomes.

The quantum threat represents a "harvest now, decrypt later" strategy where adversaries collect encrypted data today, knowing they can unlock it when quantum technology advances.⁸⁵ This shows that current data protection measures might already be inadequate for information needing long-term confidentiality. Organizations must start using quantum-resistant cryptography now instead of waiting for threats to emerge.

The development of bioware using AI to assess racial traits and predict behaviors during crises illustrates how emerging technologies introduce new threats. This approach needs access to demographic and health data, making data protection essential not just for privacy but also to prevent abuses of advanced technologies.

Institutional Framework and Governance

Multi-Stakeholder Governance

The governance framework shows complex institutional arrangements with many stakeholders across government, military, private sector, and academic institutions. The Government of India plays a key role in setting policy and legal standards. However, successful implementation requires collaboration with military bodies (due to national security needs), private companies (as technology developers and service providers), and universities (for research and workforce development).

Various committees, study groups, and working bodies suggest thorough consultation processes that aim to include diverse perspectives and expertise. The framework stresses that data players should have clear roles and responsibilities, with accountability mechanisms in case of failures. Railway ticketing security failures serve as warning signs of what can happen if governance structures are weak.

Establishing clear authority while enabling necessary information sharing and cooperation presents a significant organizational challenge. The decentralized structure of Indian infrastructure has both strengths and weaknesses. Each department has its own IT and cybersecurity frameworks and system ownership. This decentralization can prevent cascading failures but complicates ensuring that adequate expertise exists at every level for every organization managing digital infrastructure.

Public-Private Partnerships

Organizations often skip conducting vulnerability assessments and penetration tests due to external pressure. VIPs demand websites launch within three days, often with ultimatums threatening jobs. This urgency forces teams to launch sites without security audits, with promises to complete tasks that often do not happen. Cyber attacks inevitably follow. CISO positions often exist as part-time roles held by bureaucrats instead of being full-time jobs. Cyber Crisis Management Plans exist but are frequently outdated and lose relevance.

Regular assurance mechanisms for sharing best practices across organizations are often missing. Each company handles problems independently instead of learning from collective experiences. A case where a major UK firm was unable to produce for 2-3 months because of cyberattacks illustrates that data protection failures harm entire economic ecosystems, not just individual businesses, affecting supplier networks and necessitating government intervention.

Major technology firms and infrastructure providers should help design security frameworks, offering specialized knowledge. University research support is key to developing cutting-edge security technologies and training future cybersecurity professionals. However, coordination efforts and trust-building mechanisms are not well developed, hindering potentially transformative collaborative security initiatives.

Think Tanks and Policy Advocacy

The growth of the Centre for Knowledge Sovereignty highlights the role of think tanks in shaping national discussions. Operating without marketing budgets or aggressive promotion, CKS gained influence through substance instead of visibility. The organization focused on data issues long before "data" became a buzzword, coining "data sovereignty" when that idea felt radical.

Their approach includes gathering practitioners who understand realities, listening carefully, and forming independent opinions afterward. This method acknowledges that those who manage functions and technologies understand future directions better than policy theorists. The role involves collecting insights, understanding implications, and developing policy recommendations based on shared knowledge instead of isolated expertise.

The publication of "Data Sovereignty: The Pursuit of Supremacy" marked a significant milestone, reaching military establishments, parliament, leading educational institutions, and corporate libraries, creating common reference points for discussions. With over 40,000 copies distributed nationally and abroad, it established a systematic approach to thinking about data sovereignty.

Follow-up initiatives like "Thus Speaks General" (talks on geopolitics by foreign service officers, ambassadors, and military generals), "Grand Gurus" (mentorship in technology and policy from corporate leaders and senior officials), and regular roundtables support ongoing dialogue between practitioners, policymakers, and strategists.

Vision 2047 and the Path Forward

Strategic Objectives

The Vision 2047 framework outlines India's long-term plan for data governance and digital infrastructure, placing these capabilities at the center of national growth by the century mark of independence. The vision recognizes that by 2047, data will cross traditional geographic and political boundaries, acting as both currency and strategic asset in global matters.

Concerns about privacy and security are seen as vital to this vision, not just hurdles to overcome. Establishing data centers within India's borders ranks as a priority, with calls for policies mandating local data storage, backup processing within Indian jurisdiction, and building national database infrastructure. These actions aim to keep crucial data assets under Indian control.

The implementation roadmap includes several components: setting up physical infrastructure like data centers across India to ensure redundancy and accessibility; developing digital aspects such as software platforms, analytics capabilities, and interoperability standards; creating responsibility frameworks that clearly define which entities control different data types and when data can be accessed or shared.

The notion of data as "currency" by 2047 suggests recognition that data has intrinsic value that can be harnessed for economic benefits. Access to information and the ability to process and analyze data efficiently are seen as essential for economic growth and global competitiveness. Countries with superior artificial intelligence and data processing capabilities might draw economic value from India's data without returning equivalent benefits.

Implementation Challenges

Historical perceptions of India as a "third world" country with limited resources highlight the extent of change required. Building robust data systems needs significant financial investment, technical expertise, institutional capacity, and ongoing political commitment, all sustained over years to meet Vision 2047 goals.

Specific technical challenges include creating systems that can manage large volumes of transactions (hundreds of thousands to millions daily) while ensuring security, reliability, and performance. Examples from railway systems show that even crucial systems can face major security and operational issues, indicating that achieving comprehensive cybersecurity across all essential infrastructure will need continued effort and resources.

Coordination challenges are considerable. Effective data governance requires alignment among central government ministries, state governments, military and intelligence agencies, private firms,

and civil society groups. Each stakeholder contributes different perspectives, priorities, and capabilities to discussions. The mixed structure of Indian infrastructure creates both opportunities for resilience through redundancy and challenges in maintaining consistent security standards.

Mission mode programs create urgency, allocate resources, and promote cooperation that scattered initiatives cannot achieve. The scale and critical nature of the cybersecurity challenge need such focused efforts. Approaching research funding bodies and the Principal Scientific Advisor's office for cybersecurity-focused mission mode programs indicates recognition that incremental measures alone will not suffice.

Economic Dimensions

Throughout discussions, economic analysis positions data as fundamental to success in the 21st-century global economy. The talk of risks tied to economic exploitation points out vulnerabilities from relying on foreign data infrastructure and analytics. This reflects historical patterns of resource extraction, applying them to the digital space where traditional ideas of territorial sovereignty fall short.

A data-driven economy requires strong systems for data commercialization, digital transaction infrastructure, and intellectual property protection. Private businesses need clear guidelines for responsible data use that encourage innovation while respecting privacy and security needs. Involving major technology firms and platform providers is key to building competitive capabilities, but this involvement must be structured to safeguard Indian interests.

India's ambition to become a \$5 trillion economy depends on critical code and data that power every economic engine, from finance to power grids to logistics. Current trends suggest achieving this target by 2027 and possibly reaching a \$30 trillion economy by 2047 if growth patterns persist. The concepts of Digital Public Infrastructure developed during G20 illustrate India's capacity to meet both domestic and global needs.

Cultural Framing and National Pride

Efforts to connect technological progress to broader cultural narratives include linking Indian history and mythology to ideas about virtual reality and quantum computing. This connection may achieve multiple goals: nurturing national pride in technological accomplishments, showing that India has philosophical foundations for dealing with complex tech ideas, and creating cultural ties to technical initiatives that might otherwise seem abstract or foreign.

This cultural approach may help secure public support for significant investments in data infrastructure and governance by aligning them with Indian traditions instead of merely imitating Western models. References to quantum computers connect to broader ambitions for India to achieve technological leadership rather than relying on foreign innovations.

Data protection should prioritize citizens over convenience. Citizen-centered data protection helps build strong foundations for securing national data and encouraging cyber resilience. Control

matters more than physical location—if Indian embassy data is outside India, effective control determines real sovereignty.

Moving Forward

India's cyber resilience tells a story of both progress and vulnerability. The journey requires using existing knowledge while continuously learning and adapting. By moving forward with visible steps, the journey can be successfully completed—like driving at night when you can only see as far as your headlights shine, but with that limited visibility, you can complete the entire drive.

Legal integration and capacity-building efforts are crucial. Research and development must work together with action instead of remaining separate to speed up progress. Ongoing investment is needed in areas like threat detection research, AI-driven predictive modeling, incident response studies focusing on quick detection, zero-trust infrastructure research, quantum-resistant cryptography, privacy-preserving computing, and sovereignty frameworks.

The choices made today will shape the world for future generations and must secure the next 50 years. India must develop enough expertise to protect every department, every user organization, and every infrastructure system. The scale appears daunting, but the need for solutions is clear. Through teamwork, strategic planning, and ongoing commitment, India can create the resilient, sovereign digital infrastructure essential for its future prosperity and security.

Analysis

As India accelerates its digital transformation to meet its Vision 2047 goals, the country faces a more complex cybersecurity landscape that endangers both its economy and national security. The combination of rapid digital growth, geopolitical tensions, and advanced cyber threats has made data resilience a key strategic priority. This section examines India's current data resilience status, identifies key gaps and weaknesses, and draws on global best practices to inform policy recommendations. The assessment builds on findings from recent discussions on data sovereignty held by the Centre for Knowledge Sovereignty, as well as key government reports and international standards.

Data resilience, the ability of digital systems to withstand disruptions, respond to threats, and recover quickly from incidents, has become essential to national competitiveness in the 21st century.⁸⁶ For India, which aims to become a \$5 trillion economy and grow into a technology hub, strong data resilience is not merely a defensive measure. It is vital for supporting economic growth, safeguarding essential infrastructure, and maintaining strategic independence.

India's Current Data Resilience Posture

Progress and Achievements

India has made significant progress in building its cybersecurity infrastructure over the past decade. This represents a considerable improvement over prior evaluations, reflecting ongoing policy focus and institutional growth.

The creation of the Indian Computer Emergency Response Team (CERT-In) as the national agency for cybersecurity incident response has provided vital coordination capabilities.⁸⁷ CERT-In reported handling over 1.4 million cybersecurity incidents in 2023, illustrating both the scale of threats and the country's ability to detect them. The 26 percent drop in reported cybersecurity incidents from 2023 to 2024, despite increasingly sophisticated attacks, suggests stronger defensive capabilities and improved threat management.

India's Digital Public Infrastructure (DPI) has become a global example, particularly the Unified Payments Interface (UPI), which processed over 13 billion transactions worth about ₹20 lakh crores in March 2024 alone. The strong performance of this crucial financial system, managing millions of daily transactions without major disruptions, shows technical skill in handling high-

volume, critical systems. During India's G20 presidency, the DPI approach received international attention, with several countries interested in adopting similar models.

The enactment of the Digital Personal Data Protection Act (DPDP) in 2023 was a turning point in India's data governance efforts. While the implementation rules are still being developed, the law establishes key principles connecting data sovereignty to jurisdiction and recognizing citizens' data rights. This positions India alongside nations with comprehensive data protection laws, addressing a long-standing regulatory gap.

Institutional Framework Development

India has set up a multi-layered institutional structure for cybersecurity governance. The National Critical Information Infrastructure Protection Centre (NCIIPC), part of the National Technical Research Organisation, focuses on protecting critical sectors such as power, telecommunications, finance, and transportation.⁸⁸ The Indian Cyber Crime Coordination Centre (I4C), established in 2020, provides a platform to coordinate cybercrime responses across states and union territories.⁸⁹

The National Cybersecurity Policy 2013, while in need of updates, created baseline objectives including establishing a secure cyber environment, building trust in IT transactions, and developing cybersecurity workforce skills. Various sector-specific regulators—the Reserve Bank of India for financial services, the Telecom Regulatory Authority of India for telecommunications, and others—have issued cybersecurity directives suited to their areas.⁹⁰

Recent developments include forming the Defence Cyber Agency to bolster military cyber capabilities and expanding sector-specific Computer Emergency Response Teams (CERTs) covering financial services, power, and other vital sectors. This focused approach allows for specialized knowledge while maintaining coordination through CERT-In.

Technical Capabilities and Infrastructure

India's cybersecurity technical skills have grown significantly. The use of AI-powered threat detection systems during Operation Sindoor in 2020, which successfully defended against large-scale denial-of-service attacks peaking at 80-90 million hits per second, showcased sophisticated defensive abilities. Government agencies deployed red teams, advanced analytics, and international threat intelligence sharing to ensure system availability during this critical time.

The cybersecurity industry in India has matured, with many domestic firms providing specialized services in penetration testing, security operations centers, threat intelligence, and incident response. However, the sector still relies heavily on foreign technology for core security products, including endpoint protection, network security devices, and essential operating systems.

The rollout of the Aadhaar digital identity system, covering over 1.3 billion residents, represents a significant technical achievement and a vital resource needing protection. The DigiLocker system, which has issued over 175 million documents, also shows capability in managing extensive digital credential infrastructure.

Gaps and Vulnerabilities

Critical Infrastructure Vulnerabilities

India's critical infrastructure presents numerous serious vulnerabilities that could trigger wide-ranging economic and security risks.

The growing digitalization of the transportation sector, covering 6.62 million kilometers of roads, smart traffic management systems, and automated freight corridors, creates extensive opportunities for attacks. All road infrastructure is geotagged with precise location data, raising concerns about potential adversarial access to sensitive information. In times of conflict, this data could facilitate targeted strikes on bridges, tunnels, and logistics choke points without traditional reconnaissance.

Operational Technology (OT) systems in sectors like power generation, oil and gas, and manufacturing show particularly deep vulnerabilities. These systems are often 30-40 years old, designed without cybersecurity in mind, and receive updates every 20-40 years, while IT systems are refreshed every 3-5 years. The merging of IT and OT across industries lacks standardized security guidelines, with organizations conducting integration without sufficient support, leaving critical infrastructure exposed.

The healthcare sector also shows worrying vulnerability. The September 2022 AIIMS ransomware attack, which disrupted operations across a network of 17,000 computers serving 100 organizations, highlights the sector's risk. Healthcare records have become more valuable targets than financial data worldwide, yet many Indian healthcare institutions lack cybersecurity maturity models and sufficient resources for protection. A 15-day recovery period for a top institution showcases the deficiencies in forensic capabilities and business continuity planning even in leading organizations.

Human Capital and Awareness Deficits

India faces a significant shortage of roughly 500,000 to 2 million cybersecurity professionals, depending on estimates, limiting its ability to secure the expanding digital infrastructure. This skills gap is evident in many areas: a lack of trained personnel, insufficient specialized expertise, and a shortage of strategic leaders who can translate technical needs into business and policy contexts.

The human vulnerability factor remains one of the most exploited weaknesses. This behavior continues even in tech-savvy organizations, suggesting that periodic awareness training alone is not enough without a deep cultural shift that ingrains security consciousness into daily practices.

The professionalization of cybersecurity roles is still a work in progress. Chief Information Security Officer (CISO) positions are often part-time roles undertaken by bureaucrats rather than full-time roles held by certified professionals. Unlike medical or legal fields with mandatory ongoing education and professional certifications, cybersecurity practitioners do not face such standardized requirements, resulting in varying levels of competence in key positions.

Educational institutions have been slow to include cybersecurity in their curricula on a large scale. Although elite institutions offer specialized programs, the broader educational environment does not consistently build cybersecurity awareness from primary education through higher education. Data protection and digital hygiene receive little attention in general education, leaving citizens unprepared to safeguard their personal information or identify threats.

Technology Dependencies and Indigenous Capability Gaps

India's reliance on foreign technology for foundational digital infrastructure creates strategic vulnerabilities that adversaries can exploit during conflicts or diplomatic crises. The absence of domestic operating systems, domain name systems, and comprehensive geographical information systems means that adversaries could potentially control or compromise the technological base on which India's digital ecosystem relies.

The Nayara Energy incident, where a Western cloud provider cut services due to the Russia-Ukraine tensions despite the Indian company's legitimate operations, highlighted the risks of data being weaponized. Even when data is hosted within India, foreign control over underlying software platforms, management dashboards, and administrative access undermines true sovereignty. Organizations believe their data is secure because it is stored domestically, yet operational control frequently resides abroad.

The cloud-first and Software-as-a-Service models widely adopted over the past three years have introduced new vulnerabilities. Major technology platforms based overseas can access, control, or cut service to Indian organizations regardless of where the data is physically located. Simple scenarios, like manufacturers retaining remote shutdown abilities for aircraft or vehicles, exemplify how technology dependencies create leverage points for external actors.

The lack of domestic artificial intelligence models tailored to Indian needs, languages, and requirements means reliance on systems developed elsewhere, reflecting different values, priorities, and possibly embedded biases or backdoors. As AI becomes vital for both economic activities and security operations, this dependency poses a growing strategic vulnerability.

Regulatory and Coordination Gaps

Though the DPDP Act was enacted in 2023, its implementation is still incomplete, with rules under development, causing legal uncertainty for organizations working on compliance. The Act demands an independent Data Protection Board with real autonomy, but this body has not yet been set up, leaving no authority to provide guidance, settle disputes, or enforce laws.

Coordination issues among various regulatory bodies—CERT-In, NPCI, SEBI, RBI, TRAI, and sector-specific regulators—create fragmented requirements that organizations find difficult to navigate. The lack of integrated standards leaves CISOs with unclear strategic and operational guidance, prompting each organization to create its own interpretations and approaches, which misses chances for collective progress and results in inconsistent protections across sectors.

Cross-border data transfer regulations remain ambiguous, with unpublished restricted country lists, complicating international operations, especially for startups and small businesses. This regulatory confusion leads to legal costs and uncertainty, putting Indian firms at a disadvantage in global markets while not delivering clear security benefits.

The decentralized nature of Indian digital infrastructure, with each department and organization managing its own IT and cybersecurity protocols, leads to varied capabilities and coverage. While this decentralization can prevent cascading failures, it raises questions about India's ability to develop enough expertise at every level for every organization overseeing critical digital infrastructure. The scale is daunting, with thousands of organizations managing sensitive systems but lacking sufficient resources or specialized knowledge.

Systemic Process Failures

In addition to technical and human factors, systemic process failures weaken resilience. Organizations often skip vulnerability assessments and penetration testing due to pressure for quick deployment. High-priority demands for websites to launch in just three days, often with threats to careers, lead teams to go live without security checks. Promised post-launch security reviews frequently do not happen, leaving systems vulnerable from the start.

Procurement processes that focus on the lowest bidders for security solutions instead of assessing effectiveness lead to false economies. Organizations implement security measures to meet compliance standards rather than gain real protection—this "tick-box" mentality results in documentation without capability. Cyber Crisis Management Plans exist but often fall out of date, remaining five or six years old, rendering them irrelevant as threats and systems evolve.

Business Impact Analysis (BIA) and Business Continuity Planning (BCP) are crucial for building resilience, yet they often receive insufficient attention. Many organizations do not clearly understand their critical assets, acceptable recovery time frames (RTO), and permissible data loss thresholds (RPO). Without this foundational work, protection efforts become unfocused and recovery plans fall short.

International Comparisons and Best Practices

Comparative Assessment of Data Protection Frameworks

The European Union's General Data Protection Regulation (GDPR), put into effect in 2018, serves as the most thorough data protection framework in the world and has influenced laws globally. GDPR sets strict rules for data processing, requires breach notifications within 72 hours, and imposes hefty penalties of up to 4 percent of global annual revenue or €20 million, whichever amount is greater. The regulation applies to any organization processing data of EU citizens, regardless of its location, creating a de facto global standard.

India's DPDP Act shares similar philosophical views with GDPR by recognizing individual data rights and requiring consent for processing, but it differs in scope and enforcement. GDPR provides detailed rules about data processing bases, special categories of data, data subject rights,

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

and processor obligations, offering clearer guidance than India's principles-based approach. However, the complexity of GDPR has led to compliance challenges, especially for small businesses, suggesting that India's simpler framework may be more practical if properly implemented.

The United States uses a sector-based approach instead of a comprehensive federal data protection law. This includes sector-specific laws like HIPAA for healthcare and GLBA for financial services, along with state-level regulations such as California's Consumer Privacy Act. This fragmented system complicates compliance but allows customized requirements for different contexts. India's hybrid model, with the DPDP Act providing basic protections along with sector-specific regulations, may offer benefits over strictly uniform or purely sectoral approaches.

China's Personal Information Protection Law (PIPL), effective from 2021, sets detailed requirements, including data localization mandates for critical infrastructure and limits on cross-border transfers. While China's approach emphasizes state security and control over individual rights compared to democratic frameworks, its focus on data localization and domestic processing matches concerns raised in discussions in India.

Institutional Models and Governance Structures

Singapore's Cyber Security Agency (CSA), created in 2015 as a separate statutory board, provides a unified command structure for the national cybersecurity strategy, operations, and capacity building. This centralization contrasts with India's distributed model across various agencies. Singapore's method allows for clearer accountability, quicker decision-making, and more coherent policy implementation, though it requires considerable resources and political will to create such centralized authority.

The United Kingdom's National Cyber Security Centre (NCSC), part of the GCHQ intelligence agency, combines government cybersecurity functions with private sector support. It offers authoritative guidance, threat intelligence, and incident response coordination. NCSC's communication with the public, easily accessible guidance documents, and active outreach to industry have fostered trust and cooperation that surpass traditional government-industry relations. India could gain from similar public-facing expertise that combines authoritative knowledge with accessible communication.

Estonia's approach to digital resilience emerged from the 2007 cyberattacks that crippled both government and private systems, focusing on redundancy and data embassies. Estonia keeps data backups in Luxembourg while still under Estonian jurisdiction, ensuring government continuity even if domestic systems are compromised. This model offers intriguing possibilities for India but would require identifying reliable partners and ensuring real control rather than superficial arrangements.

Israel's model integrates military cyber capabilities with civilian applications through mandatory service, creating a large pool of cyber-trained personnel who transition into the private sector,

leading to deep expertise throughout the economy. While India's compulsory service framework is different, initiatives that connect defense cyber capabilities with civilian applications could increase the spread of expertise and make better use of military investments for wider economic benefits.

Technical Standards and Resilience Metrics

The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework provides commonly accepted standards for identifying, protecting, detecting, responding to, and recovering from cyber incidents. This risk-based, flexible framework lets organizations customize their implementation while following recognized best practices. Currently, India lacks similar authoritative standards, with organizations developing their approaches without unified guidance.

International standards, like ISO 27001 for information security management systems, offer certification frameworks that allow organizations to show adherence to recognized practices. However, certification alone is not enough without real implementation. The "compliance vs. capability" gap seen in Indian organizations also exists globally, though it varies in extent.

Resilience metrics used worldwide provide benchmarks that India could adopt. Mean Time to Detect (MTD) of under one hour and Mean Time to Respond/Return (MTR) of under 72 hours are globally recommended targets that India could formalize into standards. Currently, the lack of standardized metrics stops meaningful assessment of organizational capabilities and comparative benchmarking across sectors.

Workforce Development Approaches

Several countries have been creative in addressing cybersecurity skills shortages. The United Kingdom's CyberFirst program engages students from age 11 through university with cybersecurity competitions, summer schools, and bursaries, building a pipeline of future professionals.

Australia's Academic Centres of Cyber Security Excellence network connects universities with industry and government, promoting research collaboration, workforce development, and knowledge transfer. Establishing similar structures in India could speed up transforming research into practice and ensure academic programs meet industry needs.

Some countries require cybersecurity certification for government roles and critical infrastructure positions. India could implement similar requirements to ensure minimum competency standards for roles where insufficient expertise could create national vulnerabilities. Professional development requirements comparable to those in medicine or law would help maintain and upgrade skills as threats change.

Public-Private Partnership Models

The Netherlands' National Cyber Security Centre works as a partnership between the government and the private sector, with industry seconding employees to work alongside government staff.

This collaboration builds trust and shares expertise. Such a model keeps policy grounded in operational realities while giving industry insights into government priorities and capabilities.

Information Sharing and Analysis Centers (ISACs) in the United States and other nations enable sector-specific threat intelligence sharing among competitors who understand the benefits of collective security. India's fragmented approach, where organizations protect their data in isolation instead of sharing threats and defenses, misses out on opportunities to strengthen collective security. Establishing trusted frameworks for information sharing without risking competitive disadvantage could significantly boost collective defense.

Emerging Technology Governance

The EU AI Act, the first comprehensive AI regulation in the world, creates risk-based requirements for AI systems. It includes prohibited applications, high-risk systems that require strict oversight, and limited regulation for low-risk applications. As India develops its AI governance frameworks, the EU approach can provide insights on balancing innovation and risk mitigation, but India must ensure its frameworks fit its unique context and priorities rather than simply copying external models.

Quantum-safe cryptography initiatives in the United States, where NIST has standardized post-quantum cryptographic algorithms, show proactive preparation for emerging threats. Discussions in India recognize quantum threats but lack concrete preparation programs. The risk of current data facing future compromise without quantum-resistant protections is a pressing concern.

Synthesis and Path Forward

India's journey toward data resilience shows significant progress but also continuous and emerging vulnerabilities. Achieving Tier 1 GCI status and developing strong digital public infrastructure highlight capabilities and commitment. However, major breaches, critical infrastructure weaknesses, limited human capital, technology dependencies, and coordination gaps indicate that much work is left to reach the goals set for Vision 2047.

International comparisons reveal that India's challenges are not unique; every nation faces cyber threats, skill shortages, and technology dependencies. However, India's size, stage of development, geopolitical context, and aspirations present a particularly complex set of challenges. The country cannot simply adopt frameworks from smaller or wealthier nations or those with different governance systems. Instead, India must blend global best practices with local innovation, cultural strengths, and specific realities.

Need for a National Data Resilience Doctrine

The most important recommendation from this analysis is the urgent need for the Union government to introduce a National Data Resilience Doctrine. This doctrine should be the main document that brings together India's scattered cybersecurity efforts, sets clear national goals, and provides official guidance for all sectors and levels of government.

There are several strong reasons for creating such a doctrine. First, India currently runs with various uncoordinated policies, including the National Cybersecurity Policy 2013 and sector-specific rules from RBI, SEBI, TRAI, the DPDP Act 2023, along with multiple CERT-In directives. This creates confusion for CISOs, who lack clear strategic guidance. A unified doctrine would create clear structures, resolve conflicts, and offer a single source of authority.

Second, the lack of standardized resilience metrics across sectors makes it hard to assess national readiness. The doctrine should require specific, measurable goals, such as a Mean Time to Detect of under one hour and a Mean Time to Return of under 72 hours. These targets should apply across critical infrastructure, promoting accountability and allowing for progress tracking toward Vision 2047 goals.

Third, examples from other countries show the importance of national doctrines. The United States' National Cyber Strategy gives clear policy guidance. Singapore's Cybersecurity Strategy provides sector-specific plans for implementation, and Estonia's digital resilience framework helped it recover from severe attacks in 2007. India, with its unique civil-military governance and federal structure, needs a doctrine suited to its own context. This doctrine should connect civilian and defense cyber efforts while respecting state autonomy.

Fourth, the doctrine would clarify institutional responsibilities. Right now, when breaches happen, like those involving BSNL, AIIMS, or Star Health Insurance, responsibility is unclear and shared among many agencies. The doctrine should assign lead agencies for particular threats, set up escalation protocols, and create ways for the government to respond collectively to national-level cyber crises.

Fifth, a formal doctrine would elevate data resilience to an essential part of national security rather than just a technical issue. By promoting the doctrine at the highest political level, ideally through Cabinet approval and a presentation to Parliament, the government would show its commitment, gather resources, and ensure ongoing focus despite political changes.

The doctrine should include five main pillars: plans for developing indigenous technology with specific timelines and investment commitments; workforce development targets, including the vision for "million cyber karma yogis" with implementation plans; frameworks for public-private partnerships to facilitate trusted information sharing; governance for emerging technologies that covers AI security and quantum-resistant cryptography; and principles for international cooperation that balance sovereignty with the need for cross-border data sharing.

Implementing the DPDP Act

First, implementing the DPDP Act with empowered institutions, clear guidance, and enforcement mechanisms must move forward quickly. The current regulatory ambiguity undermines both compliance and protection. Second, India must systematically tackle its human capital issues through education reform, professional certification, and large workforce development programs. The "million cyber karma yogis" vision needs solid implementation strategies.

Third, indigenous technology development for foundational digital infrastructure should receive ongoing priority and investment, recognizing this as a long-term effort that requires perseverance despite setbacks. Fourth, resilience standards that establish metrics, maturity models, and sector-specific requirements could replace the current ad-hoc approaches, offering organizations clear guidance. Fifth, public-private partnerships that enable trustworthy information sharing, collective defense, and resource pooling could enhance limited resources and expertise significantly.

The path to 2047 requires India to use existing knowledge while also learning and adapting. The idea of driving at night fits well. By taking steps based on what is visible and expanding understanding through action and learning, India can successfully pursue digital sovereignty and resilience. The roundtable discussions show that expertise, commitment, and understanding exist within India's institutions, industry, and civil society. By harnessing this collective wisdom through coordinated action, India can convert current vulnerabilities into future strengths, positioning itself as both a beneficiary and contributor to global digital security.

Recommendations



Strategic Priorities and Immediate Actions

India's data resilience challenge is no longer defined by the absence of security controls, but by the **ability to recover critical systems quickly, safely, and with confidence under disruption**. As digital infrastructure becomes foundational to economic activity, governance, and citizen trust, resilience must be treated as a **measurable national capability**, not a collection of isolated initiatives.

The strategic priorities outlined below are therefore designed to **institutionalize recovery readiness**, reduce systemic fragility, and ensure continuity of essential services even when preventive controls fail. These actions build directly on the maturity progression described earlier in this report, translating resilience principles into **governable outcomes**.

Establishing a National Data Resilience Doctrine

Establishing a National Data Resilience Doctrine

A National Data Resilience Doctrine is required to unify India's fragmented cyber, data protection, and continuity efforts into a **single outcome-oriented framework**. Unlike earlier policies that emphasized prevention and compliance, the doctrine must focus on **recoverability, continuity, and confidence**, recognizing that disruption is inevitable in complex digital systems.

The doctrine should define:

- **Target resilience outcomes** (acceptable downtime, data loss, and service degradation)
- **Minimum maturity expectations** for organizations operating critical digital infrastructure
- **Standardized resilience metrics** that enable objective assessment across sectors

This approach shifts national preparedness from *policy intent* to *operational assurance*, ensuring that resilience is not assumed but **continuously demonstrated**.

India needs a National Data Resilience Doctrine that goes beyond traditional cybersecurity methods to tackle the complex issues of protecting digital infrastructure in a more threatening environment. This doctrine should rest on five key pillars that direct all policies, institutions, and technical actions across government, critical infrastructure, and the private sector.

Five Pillars of the Doctrine

The doctrine should rest on five interdependent pillars, each mapped to a core dimension of data resilience maturity:

1. Prevention and Protection (Foundation)

Focused on reducing attack surface and preserving data integrity, while explicitly recognizing that prevention alone cannot guarantee continuity.

Maturity Expectation

At higher maturity, prevention and protection reduce risk but do not create false confidence. Controls are designed to **preserve data integrity and limit blast radius**, while assuming that some attacks will succeed. Protection mechanisms directly support recoverability by ensuring that trusted data remains available for restoration when needed.

2. Detection and Response (Time Advantage)

Designed to minimize Mean Time to Detect and limit blast radius, enabling faster transition from incident to recovery.

Maturity Expectation

As maturity increases, organizations move from delayed discovery to **rapid, reliable detection** that provides time advantage. Detection capabilities are measured, continuously improved, and tightly integrated with recovery workflows, enabling faster transition from incident recognition to service restoration.

3. Recovery and Continuity (Outcome Assurance)

The core of national resilience, ensuring that critical services can be restored within defined RTO and RPO targets using **verified, trusted data**, even when primary environments are compromised.

Maturity Expectation

At advanced maturity, recovery is **predictable, repeatable, and validated**. Critical services can be restored within defined objectives using clean, trusted data, even when production environments or control systems are compromised. Recovery performance is measured, tested regularly, and treated as the primary indicator of resilience.

4. Adaptation and Evolution (Maturity Advancement)

Embedding continuous improvement through testing, automation, and learning, allowing organizations to progress from reactive recovery to **predictable, repeatable resilience**.

Maturity Expectation

Higher maturity organizations institutionalize learning by embedding **continuous testing, automation, and improvement** into normal operations. Resilience capabilities evolve

proactively in response to emerging threats, architectural change, and lessons from incidents, allowing progression from reactive recovery to assured continuity.

5. Governance and Accountability (Sustainability)

Providing oversight, measurement, and leadership visibility so that resilience is treated as a **strategic responsibility**, not a technical afterthought.

Maturity Expectation

At maturity, governance focuses on **outcomes rather than tools**. Leadership has visibility into resilience performance through standardized metrics, regular reporting, and independent validation. Accountability is tied to recovery capability and service continuity, ensuring resilience remains a sustained strategic priority.

The first pillar sets out “Prevention and Protection” through active threat intelligence, solid security systems, and ongoing vulnerability management. This includes the required implementation of zero-trust frameworks across government networks by 2028. All critical infrastructure operators must achieve security certification within three years and develop local technology capabilities to lessen reliance on foreign-controlled platforms. Organizations overseeing essential systems should conduct thorough security audits every two years and report findings to sector regulators and the proposed National Data Resilience Authority.

The second pillar emphasizes “Detection and Response”, understanding that prevention cannot eliminate all threats. India should enact standardized resilience metrics, including Mean Time to Detect (goal: under one hour), Mean Time to Respond (goal: under four hours), and Mean Time to Recover (goal: under 72 hours). The National Cyber Range should provide realistic training environments for organizations to test their incident response plans against simulated advanced attacks. Sector-specific Information Sharing and Analysis Centers must facilitate trusted sharing of threat intelligence among organizations while preserving competitive concerns and reputational issues.

The third pillar focuses on “Recovery and Continuity”, ensuring that critical systems can quickly recover after attacks or infrastructure failures. This requires the establishment of distributed national data centers with geographic redundancy across six zones, the implementation of detailed backup and disaster recovery protocols with clear Recovery Time Objectives and Recovery Point Objectives, and the creation of redundant operational capabilities that maintain essential functions even when primary systems fail. The doctrine mandates that all government services and critical infrastructure have tested business continuity plans updated every year.

The fourth pillar deals with “Adaptation and Evolution”, recognizing that threats are always evolving and defensive measures need to keep up. This includes starting the quantum-safe

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

cryptography program to defend against new quantum computing threats, setting up a network of 25 Academic Centres of Cybersecurity Excellence for leading-edge research and skill development, and launching the "Cyber Karma Yogi" National Service Corps to provide 5,000 trained professionals each year. Research and development must center on AI-driven predictive threat modeling, innovations in zero-trust infrastructure, quantum-resistant cryptography, privacy-preserving computing techniques, and sovereignty frameworks that balance openness with security.

The fifth pillar defines "Governance and Accountability", establishing clear institutional frameworks with specified responsibilities, coordination, and enforcement capabilities. The proposed National Data Resilience Authority should oversee policy across various agencies while the empowered Data Protection Board implements the Digital Personal Data Protection Act with clear guidance and consistent enforcement. Unified compliance frameworks need to combine requirements from multiple regulators, easing the burden on organizations while ensuring complete protection. Professional certification standards for cybersecurity positions should match those in medical and legal fields to guarantee minimum proficiency in roles that could otherwise create national vulnerabilities.

Recovery and Continuity

Recovery capability represents the **true test of resilience maturity**. National continuity cannot depend on assumptions that systems will remain available or that attacks can always be prevented. Instead, critical services must be architected to **resume operations rapidly using clean, validated data**.

This requires:

- Recovery architectures that operate independently of compromised production systems
- Regular validation that backups are recoverable within defined objectives
- The ability to restore services across environments without dependency on a single platform or control plane

Annual continuity plans are insufficient. Recovery readiness must be **continuously tested and measured**, ensuring that declared objectives reflect actual operational capability.

Governance and Accountability (Metrics-First)

Effective governance depends on **measurability**. Without standardized resilience metrics, neither regulators nor leadership can distinguish between perceived readiness and actual capability.

The doctrine should therefore mandate:

- Common national resilience indicators (e.g., recovery time achievement, clean recovery success rates)
- Periodic resilience reporting to organizational and sector leadership
- Independent validation of recovery capability for critical infrastructure operators

By tying accountability to **recovery outcomes rather than tool deployment**, governance mechanisms reinforce maturity progression and prevent resilience from becoming a purely compliance-driven exercise.

Establish a Unified National Data Resilience Authority

India needs a unified structure to address the existing fragmentation among different agencies and regulators. Inspired by Singapore's successful Cyber Security Agency model, India should create a National Data Resilience Authority (NDRA) as an independent body reporting directly to the Prime Minister's Office. This authority would bring together critical cybersecurity functions currently spread across CERT-In, NCIIPC, I4C, and various sector regulators, allowing for coordinated policy development, threat management, and incident response.

The NDRA should have three divisions: a Strategic Policy Division to handle frameworks and international relations; an Operations and Response Division for real-time threat intelligence and incident management; and a Capacity Building Division to focus on workforce training and public awareness. This setup would maintain CERT-In's operational capabilities while improving decision-making and reducing delays that hinder effective responses.

Instead of total centralization that could lead to bureaucratic inflexibility, the NDRA should serve as a coordinating body that works with existing sector-specific CERTs and regulators rather than replacing them. This would keep the necessary expertise while ensuring a unified national strategy. The authority should include personnel from industry, academia, and defense, similar to the Netherlands' approach of integrating private sector skills within government cybersecurity efforts.

Implement Mission Mode Quantum-Safe Cryptography Program

The threat from quantum computing demands immediate action, even though commercial quantum computers may still be years away. The "harvest now, decrypt later" strategy used by advanced adversaries means that data requiring long-term protection may be at risk unless secured with quantum-resistant algorithms now. India should implement a focused program, coordinated

through the Principal Scientific Adviser's office and supported by the Anusandhan National Research Foundation, to speed up the adoption of quantum-safe cryptography.

Following NIST's standardization process for post-quantum cryptography, which identified resistant algorithms in 2024, India should require quantum-resistant cryptography for all new government systems and critical infrastructure by 2027. The initiative should support local development of quantum-safe implementations tailored to Indian needs, set up testing and certification facilities, and create plans for transitioning legacy systems. Given India's strong background in mathematics and cryptography, this program could help position the country as a contributor to global quantum-safe standards.

The program should allocate ₹5,000 crore over five years to support research institutions, industry efforts, and upgrades for government systems. Priority should be given to critical areas like defense communications, financial networks, identity infrastructure, and diplomatic communications for their transition to quantum-safe technology. For reference, Estonia has already begun implementing protections for government data, showing that proactive measures are both possible and wise.

Mandate Critical Infrastructure Security Audits and Certification

The known weaknesses in railway systems, power infrastructure, telecom networks, and healthcare facilities require systematic evaluation and improvement. India should mandate complete security audits for all critical infrastructure operators, conducted by CERT-In certified auditors, with initial assessments due within 18 months and recurring audits every two years.

The audit framework should follow ISO 27001 standards adapted to Indian conditions, covering technical security controls, operational procedures, staff training, incident response, and business continuity planning. Infrastructure operators must achieve initial certification within three years, with increasing requirements based on risk assessments. Organizations that do not meet standards would face operational restrictions until they comply, ensuring that security is prioritized alongside efficiency and costs.

Special attention should be given to operational technology systems, which are often 30-40 years old, particularly in power generation, oil and gas, and manufacturing. These systems require specific OT security frameworks that differ from IT approaches. The Indian Computer Emergency Response Team should work with operators, equipment manufacturers, and international bodies like the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in the U.S. to develop sector-specific OT security standards.

Strengthening Data Protection Infrastructure

Deploy Distributed National Data Centers with Geographic Redundancy

India's data sovereignty needs physical infrastructure to ensure critical data stays within the country and is resilient against local disturbances. The government should set up a network of Tier IV certified data centers across six geographic zones. This will prevent any single natural disaster, power outage, or targeted attack from compromising national data systems.

Inspired by Estonia's data embassy concept, India should designate primary and secondary data centers in each zone, ensuring that real-time synchronization allows continuity even if one facility fails. These centers should adhere to the highest security standards, including biometric access controls, 24/7 armed security, electromagnetic shielding, and independent power sources. The total investment of about ₹50,000 crore over ten years would create infrastructure capable of hosting government systems, essential private sector applications, and serve as disaster recovery points for organizations reliant on foreign cloud providers.

The data center network should focus on strategic locations, such as one in the northeast for regional connectivity, one in the northwest for defense applications, southern and western sites for economic development, and central locations for government functions. Each facility should have enough capacity to absorb workloads from affected sister sites, ensuring genuine resilience instead of just nominal backup.

Develop Indigenous Cloud Infrastructure and Operating Systems

India's reliance on foreign technology for essential infrastructure creates strategic risks that need long-term solutions. The government should launch a National Indigenous Technology Mission, similar to the space program's goals, to develop crucial technological capabilities over the next 15-20 years.

Initial priorities should cover a secure Indian operating system based on advanced Linux versions, designed for government and critical infrastructure use; local database management systems capable of handling large-scale workloads; cloud orchestration platforms for deploying applications across domestic infrastructure; and security tools such as endpoint protection, network security, and security information management systems.

This mission should not aim to replace all foreign technology immediately, as such attempts often fail due to market dynamics and ecosystem effects. Instead, the focus should be on creating domestic alternatives for the most sensitive 20 percent of applications where foreign dependencies pose unacceptable risks. The remaining 80 percent can continue using global technology while India gradually builds its own capabilities.

The mission should utilize India's significant software engineering talent through public-private partnerships, with government funding supporting foundational research and early development, while the private sector manages commercialization and scaling. Israel's approach of blending military cyber expertise with civilian applications shows how defense investments can lead to broader economic benefits. India's defense research services, IITs, and the private sector should work closely together, with clear rules on intellectual property that ensure innovations serve national interests while benefiting contributors.

Establish Data Trusts for Sector-Specific Information Sharing

The current separation, where each organization guards its data in isolation, overlooks opportunities for collective defense and economic gains. India should create sector-specific data

trusts—legal entities managing data for multiple stakeholders under governance structures that ensure appropriate use while preventing misuse.

For example, the insurance sector, where companies keep claims data and fraud warnings separate, limits accurate risk assessments. A National Insurance Data Trust could compile claims histories, fraudulent patterns, and risk evaluations, while still allowing companies to differentiate themselves in underwriting and customer service. Similar trusts for healthcare (enabling research while protecting privacy), agriculture (weather, soil, crop data), and smart cities (traffic, utilities, public services) could speed up development while ensuring security.

These trusts should be governed strictly, including multi-stakeholder boards with representatives from contributors, users, and public interests; clear rules for data usage; strong anonymization and privacy-preserving techniques; regular independent audits; and accountability measures for breaches or misuse. The UK's Open Data Institute offers useful frameworks for data trusts that balance innovation with protection.

Implement Zero Trust Architecture for Government Networks

The traditional security model, which assumes anything inside the network is trustworthy, fails against sophisticated threats that breach perimeters through social engineering, supply chain attacks, or insider risks. India should require zero trust architecture for all government networks by 2028, in line with the U.S. federal government's zero trust strategy introduced in 2021.

India should plan to Fortify data, identity and applications with Zero Trust Resilience

India should have the capacity to recover data instantly across your hybrid estate and restore data at super speed - 4x or 5x times faster than what it can do today. India must ensure data portability, so any critical infrastructure data is never locked in and it is free to move or restore workloads. India must keep operations resilient against modern threats with immutable backups, cleanroom validation, and automated rollback to a trusted state. Data Resilience means to recover and rollback with precision, minimizing data loss and downtime through forensic-proof recovery and cross-cloud portability.

India must keep operations resilient against modern threats with immutable backups, cleanroom validation, and automated rollback to a trusted state. Data Resilience means to recover and rollback with precision, minimizing data loss and downtime through forensic-proof recovery and cross-cloud portability. Zero trust principles include verifying all data points, such as user identity, device status, location, and behavior patterns; using the least privilege access, providing users only the minimal permissions needed; and assuming breaches, designing systems to limit damage through micro-segmentation and continuous monitoring.

Implementation will need a significant investment in identity management systems, multi-factor authentication, micro-segmentation technologies, and continuous monitoring tools. However, this investment will pay off by significantly reducing attack surfaces and restricting adversaries' movement within networks. The U.S. Cybersecurity and Infrastructure Security Agency's zero trust maturity model provides a phased implementation guideline that India can tailor to its needs.

Policy and Regulatory Framework

Complete DPDP Act Implementation with Empowered Data Protection Board

The success of the Digital Personal Data Protection Act relies on how well it is implemented. The government must set up the Data Protection Board of India as an independent body with sufficient funding, legal powers, and protection from political interference. Modeled after the Reserve Bank of India's institutional independence, the Board should consist of technology experts, legal professionals, civil society members, and industry representatives selected transparently with set terms.

The Board needs to deliver several key components quickly: clear rules that clarify vague provisions; specific guidance for sectors like healthcare, finance, and telecommunications; model consent processes to help organizations comply; and certification frameworks that allow businesses to show credible compliance. These components should be developed with input from the public and stakeholders to ensure they are practical.

Importantly, the Board must have strong enforcement capabilities, including the authority to investigate, impose penalties, and enforce corrective actions. However, enforcement should be gradual, initially emphasizing guidance and capacity-building, then moving to penalties. This approach will allow organizations time to ensure they truly comply, rather than just appearing compliant.

Establish Unified Compliance Framework Integrating Multiple Regulations

Organizations currently face a confusing mix of requirements from CERT-In, RBI, SEBI, TRAI, IRDAI, and other regulators, often with overlapping or conflicting rules. The government should create a Unified Digital Compliance Framework that provides clear guidance on obligations across different regulations.

This framework should relate requirements to organizational characteristics, such as sector, size, data sensitivity, and infrastructure security. It should generate personalized compliance roadmaps. A technology platform implementing the framework could allow organizations to enter their profiles and receive tailored guidance on applicable rules, reporting needs, and timelines. Singapore's Business Grants Portal shows how technology can ease compliance.

The framework should align where possible, for instance, by establishing common definitions for personal data, security incidents, and breach notifications across regulations. Where sector-specific rules differ due to unique risks, the framework should clearly explain the reasons and provide guidance on transitions. Regular reviews should identify new conflicts or gaps that need regulatory attention.

Publish Restricted Country List and Cross-Border Transfer Framework

The DPDP Act's sections on cross-border data transfers are inactive without published lists of restricted countries and approved transfer processes. This regulatory gap significantly impacts

startups and small businesses trying to operate internationally. Larger companies often rely on costly legal advice to navigate the uncertainty.

The government should release the restricted country list within six months, based on objective criteria like the adequacy of the foreign data protection framework, India's diplomatic relationships, reciprocity in data access, and participation in international cybersecurity cooperation. The list should be reviewed annually with clear processes for updates.

For transfers to unrestricted countries, standard contractual clauses similar to those in the EU should provide legal clarity. For restricted countries where legitimate needs exist, the Data Protection Board should set up approval processes that balance economic interests and security. Cloud service providers should disclose all locations where data might be processed or accessed, including headquarters and jurisdictions that require data production.

Mandate Cybersecurity Professional Certification for Critical Roles

The voluntary approach to cybersecurity training results in inconsistent skills in positions where insufficient expertise can create national risks. India should require certification for individuals in key cybersecurity roles, similar to the standards for accountants, medical practitioners, and lawyers.

The Institute of Information Security Professionals should be established by law to create certification standards, accredit training providers, conduct exams, and maintain professional registries.

All government positions involving cybersecurity responsibilities and private sector roles in critical infrastructure or handling sensitive data should require appropriate certification within three years. Continuing professional development of 40 hours annually should be mandatory for maintaining certification, ensuring practitioners stay current as threats evolve. The UK's professional body, CREST, provides useful models for practitioner certification in cybersecurity.

Building National Capacity

Launch National Cybersecurity Education Initiative from School Level

Addressing India's shortage of cybersecurity professionals requires building foundations early rather than attempting to create expertise at higher education stages. The Ministry of Education should integrate cybersecurity and digital literacy into curricula from Class 6 onward, developed in partnership with industry and adapted to age-appropriate learning. Introducing Data Resilience Education in Schools

To achieve sustainable cybersecurity, starting from childhood is crucial. India should introduce "Data Resilience and Digital Citizenship" as a mandatory subject beginning in Class 6, incorporated into the national curriculum framework. This first-of-its-kind initiative addresses the fact that current and future generations will live in fully digitized environments, where understanding data protection, privacy rights, and cyber threats will be key to individual well-being and national security.

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

The curriculum should use age-appropriate, progressive learning methods. For Classes 6-8, foundational modules should teach digital hygiene practices like password management, recognizing phishing attempts, safe browsing, and how personal data is collected and used by applications and websites. Students would gain practical skills for protecting their digital identities while becoming aware of online risks such as cyberbullying, social engineering, and misinformation. For Classes 9-10, intermediate modules would explain privacy rights under Indian law, how digital systems work and can be compromised, the economic and social value of data, and how to critically evaluate online sources. Students would engage with case studies on data breaches, their impacts, and preventive measures that individuals and organizations should take.

For Classes 11-12, advanced modules would provide specific pathways for students interested in cybersecurity careers while ensuring that all students recognize their responsibilities as digital citizens. Topics would cover new technologies like artificial intelligence, blockchain, and quantum computing, ethical concerns around data collection and sharing, national security aspects of cybersecurity, and India's challenges and goals regarding data sovereignty. Students finishing secondary education should have practical skills to protect personal and organizational data, a conceptual understanding of India's digital infrastructure and vulnerabilities, awareness of career options in cybersecurity and data protection, and a sense of civic duty regarding their role in collective digital resilience.

The implementation strategy requires training 500,000 teachers over three years through specialized programs developed in collaboration with leading technology institutions and industry practitioners. The Ministry of Education should partner with organizations like the Centre for Knowledge Sovereignty, Indian Institutes of Technology, and cybersecurity firms to develop teaching materials, conduct workshops, and offer ongoing support. Annual national competitions, modeled after science and math Olympiads, could identify talented students for accelerated pathways like summer schools, mentorship programs, and scholarships for higher education in cybersecurity fields.

To complement formal education, public awareness campaigns should target parents, senior citizens, and working professionals who completed their education before digital threats became widespread. Mass media campaigns, community workshops, and workplace training programs should reinforce messages about digital hygiene, fraud prevention, and responsible data management. Financial institutions, telecommunications companies, and tech platforms need to participate in these efforts through customer education initiatives that go beyond meeting regulatory requirements to genuinely build capacity.

This extensive educational transformation, along with the five-pillar National Data Resilience Doctrine, professional certification standards, institutional reforms, and infrastructure investments, provides India with a clear path to achieving data sovereignty and resilience in line with Vision 2047 goals. Success depends on sustained political commitment, proper resource allocation, and the involvement of society as a whole, acknowledging that data resilience is key to whether India's digital transformation continues to foster inclusive growth and strategic independence or becomes a target for exploitation by adversaries seeking to disrupt the economy and exert geopolitical pressure.

C
E
N
T
R
E
F
O
R
K
N
O
W
L
E
D
G
E
S
O
V
E
R
E
I
G
N
T
Y

The curriculum should cover: digital hygiene practices (password management, recognizing phishing, safe browsing); privacy protection and data rights; basic understanding of how digital systems work and can be compromised; and introduction to cybersecurity careers and pathways. Advanced students should have opportunities for specialized learning through elective courses at secondary level.

Following the UK's CyberFirst program, India should establish national cybersecurity competitions, summer schools, and mentorship programs identifying talented students and providing accelerated pathways into the profession. State-level competitions feeding into national championships would create visibility and aspiration similar to how mathematics and science olympiads identify talent in those domains. Corporate sponsorship and government funding should support these initiatives as both workforce development and national security investments.

Establish Centres of Excellence on Cybersecurity, Data Sovereignty and Resilience

India should designate 25 Academic Centres of Cybersecurity Excellence distributed across states, building on Australia's successful model. These centers would serve as regional hubs for research, training, industry collaboration, and incident support, addressing the concentration of expertise in major metros while building distributed capabilities.

Each center should focus on specific domains—some specializing in industrial control system security, others in cryptography, financial sector security, healthcare security, or AI safety. This specialization creates deep expertise while ensuring the network collectively addresses all critical areas. Centers should maintain strong industry partnerships, with corporate secondments bringing practitioners into academic environments while researchers spend time in industry understanding operational realities.

The centers should operate with substantial autonomy but coordinate through a National Cybersecurity Research Consortium ensuring complementary rather than duplicative work. Annual funding of ₹500 crore (₹20 crore per center) would support faculty positions, research projects, student fellowships, and infrastructure. Expected outputs include: research publications advancing the field; trained graduates entering workforce; continuing education programs for professionals; and rapid response capabilities supporting regional organizations facing incidents.

Develop "Cyber Karma Yogi" National Service Corps

The concept of "cyber karma yogis"—professionals viewing cybersecurity as both vocation and civic duty—requires institutional expression beyond rhetoric. India should establish a National Cybersecurity Service Corps, a three-year program for recent graduates providing immersive training and practical experience defending critical infrastructure.

Participants would receive stipends comparable to entry-level private sector salaries while rotating through government agencies, critical infrastructure operators, and underserved organizations lacking security capabilities. The program would combine advanced technical training, hands-on experience, mentorship from senior practitioners, and exposure to policy and strategy

considerations. After completing service, participants would join a reserve corps, committing to support national responses to major incidents.

An annual cohort of 5,000 participants would address immediate workforce shortages while building a cadre of professionals with both technical expertise and national security consciousness. The program should partner with industry for training delivery and placement, with corporate participants receiving tax benefits for contributing instructors and hosting fellows. This model adapts AmeriCorps and Teach for America concepts to cybersecurity contexts, recognizing that addressing critical shortages requires innovative approaches beyond traditional education pathways.

Create Public-Private Information Sharing Framework

The absence of trusted mechanisms for sharing threat intelligence leaves organizations repeatedly discovering the same attacks rather than benefiting from collective experience. India should establish sector-specific Information Sharing and Analysis Centers (ISACs) following the U.S. model, with centers for financial services, telecommunications, power, transportation, healthcare, and manufacturing.

ISACs should function as industry-led organizations with government participation but private sector governance, ensuring members trust the confidentiality of shared information. They would operate secure platforms for sharing indicators of compromise, attack patterns, vulnerability information, and defensive measures. Anonymization protocols would allow sharing sensitive information without identifying affected organizations inappropriately.

To overcome reluctance to share due to competitive concerns or reputational risks, the government should provide liability protection for good-faith information sharing through legislative amendments. The CERT-In should coordinate across ISACs, identifying patterns visible only from aggregated national perspective while respecting the need for sectoral autonomy and confidentiality.

Implement Resilience Metrics and Maturity Model Framework

India lacks standardized metrics enabling organizations to assess their resilience capabilities or benchmark against peers. The Data Protection Board should develop a National Data Resilience Maturity Model, adapted from frameworks like NIST's Cybersecurity Framework and CERT-RMM, providing graduated levels from initial/ad-hoc through defined, managed, and optimizing.

The maturity model should cover five domains: governance and risk management; technical security controls; incident response and recovery capabilities; workforce competency; and supply chain security. Organizations would self-assess initially, with third-party assessments required for critical infrastructure. Maturity scores should be reported to relevant regulators, enabling supervisory focus on lower-maturity organizations requiring assistance.

Key performance indicators should include: Mean Time to Detect (target: under 1 hour); Mean Time to Respond (target: under 4 hours); Mean Time to Recover (target: under 72 hours);

percentage of systems with current security patches (target: >95%); workforce training completion rates (target: 100% annually); and simulation exercise frequency (target: quarterly). These metrics provide concrete targets replacing vague commitments to "strong security."

Establish National Cyber Range for Training and Simulation

Effective cybersecurity training requires realistic environments where practitioners can develop skills without risking production systems. India should establish a National Cyber Range—a large-scale simulation environment replicating critical infrastructure, corporate networks, and government systems where security teams can practice defense, incident response, and recovery.

The cyber range should support multiple simultaneous exercises with thousands of participants, enabling organizations to test their plans, train personnel, and validate capabilities against simulated attacks of varying sophistication. Annual competitions on the range would identify talented individuals while raising professional standards through competitive benchmarking.

Following the U.S. Department of Defense's model, the range should be available to government, critical infrastructure operators, and private sector through time-slot bookings.²² Academic institutions could use it for training programs while corporate teams conduct exercises. Red team services from the cyber range would provide organizations with professional adversarial testing, identifying vulnerabilities before real attackers exploit them.

Conclusion

Implementing these recommendations requires sustained commitment, substantial resources, and coordination across government, industry, academia, and civil society. However, the investment is essential and urgent—delays compound vulnerabilities while adversaries advance capabilities. The roadmap spans immediate actions (security audits, DPDP implementation), medium-term initiatives (data center network, certification requirements), and long-term programs (indigenous technology development, workforce transformation).

India's progress toward digital sovereignty and resilience will determine whether the nation achieves its Vision 2047 aspirations or faces constraints from technological dependencies, skills shortages, and infrastructure vulnerabilities. The comprehensive approach outlined above, drawing on international best practices while reflecting Indian contexts and capabilities, provides a practical pathway forward. Success requires treating data resilience not as a technical concern for specialists but as a national priority demanding whole-of-society engagement and resources commensurate with the stakes involved.

All government positions that involve cybersecurity responsibilities and private sector jobs in critical infrastructure or handling sensitive data should require the right certification within three years. Practitioners must complete 40 hours of professional development each year to maintain their certification. This ensures they keep up with evolving threats. The UK's professional body, CREST, offers useful models for cybersecurity certification.

India's progress towards digital independence and resilience will dictate whether the nation can achieve its Vision 2047 goals or face limitations due to technological dependencies, skill gaps, and infrastructure weaknesses. The comprehensive approach outlined here, which draws on international best practices while considering Indian contexts and capabilities, offers a practical path forward. Success depends on viewing data resilience not just as a technical issue for specialists but as a national priority that calls for widespread engagement and resources that match the significance of the challenges involved.

Endnotes

- ¹ IANS. 2025. "India on Track to Become 5 Trillion Economy by 2027: Piyush Goyal." NDTV, [Month Day]. <https://www.ndtv.com/india-news/india-on-track-to-become-5-trillion-economy-by-2027-piyush-goyal-8754940>.
- ² Press Information Bureau, Government of India. "Press Release PRID 2097125." Accessed March 9, 2026. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2097125®=3&lang=2>.
- ³ *ibid*
- ⁴ Press Information Bureau, Government of India, "As of April 2024, 95.15% Villages Having Access to Internet," accessed December 13, 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2040566>.
- ⁵ Business Standard, "UPI's Share in Total Digital Payments in India Grows to 83% in 2024," January 27, 2025, https://www.business-standard.com/finance/news/upi-s-share-in-total-digital-payments-in-india-grows-to-83-in-2024-125012701372_1.html; India Brand Equity Foundation, "United Payments Interface (UPI) Dominates Digital Payments, Sees Explosive Growth Over Five Years," January 28, 2025, <https://www.ibef.org/news/united-payments-interface-upi-dominates-digital-payments-sees-explosive-growth-over-five-years>.
- ⁶ <https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html>
- ⁷ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2123192®=3&lang=2>
- ⁸ Press Information Bureau, Government of India, "BharatNet: Bridging the Digital Divide," accessed December 13, 2025, <https://www.pib.gov.in/PressNoteDetails.aspx?NotelId=153588&ModuleId=3>.
- ⁹ Press Information Bureau, "As of April 2024."
- ¹⁰ Press Information Bureau, Government of India. "Press Release PRID 2097125." Accessed March 9, 2026. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2097125®=3&lang=2>.
- ¹¹ *ibid*
- ¹² US Department of Commerce, International Trade Administration, "India - Digital Economy," Country Commercial Guide, accessed December 13, 2025, <https://www.trade.gov/country-commercial-guides/india-digital-economy>. ↵
- ¹³ *ibid*
- ¹⁴ *ibid*
- ¹⁵ Brussels Privacy Hub, "Data Protection and Cross-border Data Flows in India Version 2.0," Working Paper Vol. 10 No. 5, March 2024, <https://brusselsprivacyhub.com/wp-content/uploads/2024/05/Data-Protection-and-Cross-border-Data-Flows-in-India-v2.0.pdf>. ↵
- ¹⁶ *ibid*
- ¹⁷ Organisation for Economic Co-operation and Development, "Cross-border Data Flows," policy brief, accessed December 13, 2025, <https://www.oecd.org/en/topics/sub-issues/cross-border-data-flows.html>. ↵
- ¹⁸ Press Information Bureau, Government of India, Ministry of Electronics and Information Technology, "India Launches First Digital Threat Report 2024 to Support Cybersecurity in the Banking, Financial Services and Insurance (BFSI) Sector," press release, February 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119801>.
- ¹⁹ Unique Identification Authority of India, "Aadhaar Authentication Surges Past 2,707 Cr in 2024-25; Aadhaar e-KYC Transactions Close to 45 Cr in March," press release, April 29, 2025, <https://www.uidai.gov.in/en/media-resources/media/press-releases/18883-aadhaar-authentication-surges-past-2-707-cr-in-2024-25-aadhaar-e-kyc-transactions-close-to-45-cr-in-march.html>; Ministry of Electronics and Information Technology, Government of India, statement cited in DD News, "Aadhaar Authentication Surpasses 2,707 Crore in FY 2024-25; UIDAI Honoured with PM's Award for Innovation," April 29, 2025,
- ²⁰ Ministry of Electronics and Information Technology (CERT-In), Government of India, "CERT-In 2022 Annual Report," cited in Business Standard, "1.39 Million Cyberattacks Handled in 2022, Phishing Attacks Rise: Cert-In," November 15, 2023, https://www.business-standard.com/india-news/1-39-million-cyberattacks-handled-in-2022-phishing-attacks-rise-cert-in-123111500614_1.html. ↵

²¹ ibid

²² World Economic Forum, "Strategic Cybersecurity Talent Framework," white paper, April 2024, <https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/>

²³ Press Information Bureau, Government of India, "Government of India Taking Measures to Protect Critical Infrastructure and Private Data Against Cyber Attacks," press release, February 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341>.

²⁴ Press Information Bureau, "India Launches First Digital Threat Report 2024."

²⁵ Securities and Exchange Board of India, "Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)," circular no. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113, August 20, 2024, <https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-85964.html>.

²⁶ Kratikal, "Navigating SEBI's 2024 Updated Cybersecurity Framework: Key Revisions," October 7, 2024, <https://kratikal.com/blog/navigating-sebi-2024-updated-cybersecurity-framework-key-revisions/>.

²⁷ SISA, "SEBI's New Cyber Resilience Guidelines Explained," October 14, 2024, <https://www.sisainfosec.com/blogs/navigating-sebis-new-cyber-resilience-guidelines-how-sisa-can-empower-your-cybersecurity-strategy/>.

²⁸ Unique Identification Authority of India, "Aadhaar Authentication Surges Past 2,707 Cr in 2024-25; Aadhaar e-KYC Transactions Close to 45 Cr in March," press release, April 29, 2025, <https://www.uidai.gov.in/en/media-resources/media/press-releases/18883-aadhaar-authentication-surges-past-2-707-cr-in-2024-25-aadhaar-e-kyc-transactions-close-to-45-cr-in-march.html>.

²⁹ OpenGov Asia, "Cyber Resilience: Securing India's Digital Landscape," March 27, 2025, <https://opengovasia.com/2025/03/27/cyber-resilience-securing-indias-digital-landscape/>.

³⁰ PRESS Insider, "India Lost \$2.64 Billion to Cyber Fraud in 2024, Govt Says," citing Global Initiative for Restructuring Environment and Management report, July 23, 2025, <https://pressinsider.com/policy/india-lost-2-64-billion-to-cyber-fraud-in-2024-govt-says/>; OpenGov Asia, "Cyber Resilience: Securing India's Digital Landscape."

³¹ Press Information Bureau, Government of India, Ministry of Electronics and Information Technology, "National Data Governance Framework Policy," press release, May 26, 2022, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1845318>.

³² Brussels Privacy Hub, "Data Protection and Cross-border Data Flows in India Version 2.0," Working Paper Vol. 10 No. 5, March 2024, <https://brusselsprivacyhub.com/wp-content/uploads/2024/05/Data-Protection-and-Cross-border-Data-Flows-in-India-v2.0.pdf>.

³³ Ministry of Home Affairs, Government of India, statement by Minister of State for Home Affairs Bandi Sanjay Kumar in Lok Sabha, July 2025, cited in Inc42, "Indians Lost INR 22,845 Cr To Cyber Fraud In 2024: Govt," July 22, 2025, <https://inc42.com/buzz/indians-lost-inr-22845-cr-to-cyber-fraud-in-2024-govt/>.

³⁴ Press Information Bureau, Government of India, "India Launches First Digital Threat Report 2024 to Support Cybersecurity in the Banking, Financial Services and Insurance (BFSI) Sector," press release, February 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119801>.

³⁵ Business Today, "How Can Exclusive Domains Like Bank.in by RBI Enhance India's Cybersecurity and Save Rs 21,367 Cr?," April 26, 2025, <https://www.businesstoday.in/industry/banks/story/how-can-exclusive-domains-like-bankin-by-rbi-enhance-indias-cybersecurity-and-save-rs-21367-cr-473737-2025-04-26>.

³⁶ Carnegie Endowment for International Peace, "Mapping India's Cybersecurity Administration in 2025," September 2025, <https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025>

³⁷ Press Information Bureau, Government of India, "Government of India Taking Measures to Protect Critical Infrastructure and Private Data Against Cyber Attacks," press release, February 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341>.

³⁸ OpenGov Asia, "India's Digital Data Protection Framework: Safety, Trust and Resilience," January 4, 2025, <https://opengovasia.com/2025/01/04/indias-digital-data-protection-framework-safety-trust-and-resilience/>. ↩

³⁹ ibid

⁴⁰ New Kerala, "22.68 Lakh Cyber Crimes, Rs 22,845 Crore Lost in 2024: Centre," December 2025, <https://www.newkerala.com/news/o/2268-lakh-cyber-crimes-registered-rs-22845-crore-lost-760>.

- ⁴¹ Ministry of Home Affairs statement, July 2025.
- ⁴² Press Information Bureau, "Government of India Taking Measures to Protect Critical Infrastructure."
- ⁴³ Ministry of Electronics and Information Technology, Government of India, "Estimation and Measurement of India's Digital Economy," report, January 2025, <https://www.meity.gov.in/content/report-estimation-and-measurement-indias-digital-economy>; Press Information Bureau, Government of India, "Future Ready: India's Digital Economy to Contribute One-Fifth of National Income by 2029-30," press release, December 11, 2024, <https://www.pib.gov.in/PressReleaselframePage.aspx?PRID=2097125>. ↵
- ⁴⁴ Vinit Goenka, *Data Sovereignty: The Pursuit of Supremacy* (Delhi: Penman Books, 2019), https://php.worldindia.in/cksindia/wp-content/uploads/2025/03/Data_Sovereignty_The_Pursuit_Of_Supremacy_watermark.pdf.
- ⁴⁵ *ibid*
- ⁴⁶ Kartik Bommakanti. "Chinese Cyber Escalation Against India's Electricity Grid Amidst the Boundary Crisis." *Observer Research Foundation*, March 10, 2021. <https://www.orfonline.org/expert-speak/chinese-cyber-escalation-india-electricity-grid-boundary-crisis> (accessed January 7, 2026)
- ⁴⁷ Nikhil Pandey. "Chinese Cyberattack That Caused the 2020 Mumbai Blackout Was a 'Warning Shot': Report." *WION News*, February 28, 2021. <https://www.wionews.com/india-news/chinese-cyberattack-that-caused-the-2020-mumbai-blackout-was-a-warning-shot-report-367125> (accessed January 7, 2026).
- ⁴⁸ Government of India, Ministry of Power. "Cybersecurity of Power Grids." Press Information Bureau, August 8, 2024. <https://www.pib.gov.in/PressReleaselframePage.aspx?PRID=2043154®=3&lang=2> (accessed January 7, 2026).
- ⁴⁹ Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India, "India Ransomware Report Year 2024," 2024, 2, https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2024.pdf.
- ⁵⁰ *ibid*
- ⁵¹ *ibid*
- ⁵² Cyber Security Asia, "Indian Industry Cybersecurity Report 2024: Trends, Insights, and 2025 Recommendations by SecureClaw," January 3, 2025, <https://cybersecurityasia.net/indian-cybersecurity-report-2024/>. ↵
- ⁵³ *ibid*
- ⁵⁴ CERT-In, "India Ransomware Report Year 2024," 3
- ⁵⁵ *ibid*
- ⁵⁶ *ibid*
- ⁵⁷ *ibid*
- ⁵⁸ 63SATS Cybertech, "India's Major Cybersecurity Incidents of 2024: What Lies Ahead in 2025," January 2, 2025, <https://63sats.com/blog/indias-major-cybersecurity-incidents-of-2024-what-lies-ahead-in-2025>.
- ⁵⁹ Carnegie Endowment for International Peace, "Mapping India's Cybersecurity Administration in 2025," September 2025, <https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025>.
- ⁶⁰ 63SATS Cybertech, "India's Major Cybersecurity Incidents of 2024."
- ⁶¹ *ibid*
- ⁶² Corbado, "10 Biggest Data Breaches in India [2025]," accessed December 20, 2025, <https://www.corbado.com/blog/data-breaches-India>
- ⁶³ "Indian blue-collar worker database, eMigrate, in the hands of hackers: Report," *The Hindu*, June 28, 2024 accessed January 7, 2026, <https://www.thehindu.com/sci-tech/technology/internet/indian-blue-collar-worker-database-emigrate-in-the-hands-of-hackers/article68343850.ece>.
- ⁶⁴ Internet Freedom Foundation, "IFF's Cybersecurity Report for the Third Quarter of 2024," November 1, 2024, <https://internetfreedom.in/iffs-cybersecurity-report-for-the-third-quarter-of-2024/>
- ⁶⁵ Corbado, "10 Biggest Data Breaches in India [2025]."
- ⁶⁶ Cyber Security Asia, "Indian Industry Cybersecurity Report 2024."
- ⁶⁷ *ibid*
- ⁶⁸ CERT-In, "India Ransomware Report Year 2024," 12.
- ⁶⁹ Carnegie Endowment for International Peace, "Mapping India's Cybersecurity Administration in 2025."

⁷⁰ *ibid*

⁷¹ PRESS Insider, "India Lost \$2.64 Billion to Cyber Fraud in 2024, Govt Says," citing Global Initiative for Restructuring Environment and Management report, July 23, 2025, <https://pressinsider.com/policy/india-lost-2-64-billion-to-cyber-fraud-in-2024-govt-says/>. ↵

⁷² 63SATS Cybertech, "India's Major Cybersecurity Incidents of 2024."

⁷³ PRESS Insider, "India Lost \$2.64 Billion to Cyber Fraud in 2024."

⁷⁴ "India's Dedicated Freight Corridor: Progress and Prospects." India Briefing, June 5, 2024. <https://www.india-briefing.com/news/india-dedicated-freight-corridor-progress-and-prospects-31860.html/>.

⁷⁵ Parliament of India. *Department-Related Parliamentary Standing Committee on Home Affairs. Two Hundred Fifty-Fourth Report: Cyber Crime – Ramifications, Protection and Prevention*. Rajya Sabha Secretariat, New Delhi, August 2025. https://www.medianama.com/wp-content/uploads/2025/08/rsnew_Committee_site_Committee_File_ReportFile_15_197_254_2025_8_12-1.pdf

⁷⁶ Estonian Ministry of Foreign Affairs. *Cybersecurity Report April 2025*. Tallinn: Estonian Ministry of Foreign Affairs, April 2025. <https://vm.ee/sites/default/files/documents/2025-08/Cybersecurity%20report.pdf>

⁷⁷ Eskhita, Radwan. *From Brussels to the Gulf: Investigating the Impact of the GDPR in UAE, Bahrain and Qatar*. PhD diss., Erasmus University Rotterdam, 2025. https://pure.eur.nl/ws/files/181895089/dissertation_-_radwan_eskhita_-_for_publication_-_679911264a60f.pdf

⁷⁸ Roy Chowdhury, Probir, and Shivani Bhatnagar. "India – Trends and Developments." In *Cybersecurity 2025*, 2025. *Chambers Global Practice Guides*. March 13, 2025. <https://practiceguides.chambers.com/practice-guides/cybersecurity-2025/india/trends-and-devel>

⁷⁹ *ibid*

⁸⁰ Bricker, Annie. "As MENA Moves to the Cloud, CIOs Look to Keep Data In-Country." *CIO*, July 22, 2019.

<https://www.cio.com/article/220394/as-mena-moves-to-the-cloud-cios-look-to-keep-data-in-country.html>

⁸¹ Roy Chowdhury and Bhatnagar, "India – Trends and Developments," *Cybersecurity 2025*.

⁸² "Make Backup and Disaster Recovery a Priority, Not an Afterthought," *iAfrica.com*, accessed January 7, 2026, <https://iafrica.com/make-backup-and-disaster-recovery-a-priority-not-an-afterthought/>

⁸³ Greg Austin, ed., *National Cyber Emergencies: The Return to Civil Defence*, 1st ed. (London and New York: Routledge, 2020), <https://doi.org/10.4324/9780429343438>

⁸⁴ Cyber Security Agency of Singapore, *Cybersecurity Education and Learning Guidebook*, <https://isomer-user-content.by.gov.sg/36/f97bc4f4-83d8-4634-90e3-5ee90fea8a22/csa-cybersecurity-education-and-learning-guidebook.pdf>

⁸⁵ Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et de Qualité des produits et services (ILNAS) and University of Luxembourg. *Big Data: White Paper, Version 1.2*. Luxembourg: ILNAS, November 2016. <https://www.coursehero.com/file/77097860/wp-bigdata-v1-2pdf/>

⁸⁶ Austen D. Givens, Nathan E. Busch, and Alan Bersin, *Homeland Security* (New York: Routledge, n.d.).

⁸⁷ CERT-In, "India Ransomware Report Year 2024," 3

⁸⁸ Carnegie Endowment for International Peace, "Mapping India's Cybersecurity Administration in 2025."

⁸⁹ Gupta, Manvi, and Ayush Gupta. "Cyber Security Legal Framework in India – Overlaps, Problems and Challenges." *Journal of Business Management and Information Systems* 12, no. 1 (March 2025): 11–20. <https://doi.org/10.48001/jbmis.1201002>

⁹⁰ Kaur, Gagandeep, Narendra N. Dalei, Sushanta Kumar Mahapatra, and Vinay Kandpal, eds. *Cybersecurity, Law, and Economics: The Case of India*. London & New York: Routledge, 2024. <https://www.taylorfrancis.com/books/edit/10.4324/9781003517290/cybersecurity-law-economics-gagandeep-kaur-narendra-dalei-sushanta-kumar-mahapatra-vinay-kandpal>



Glimpses

GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



GLIMPSES



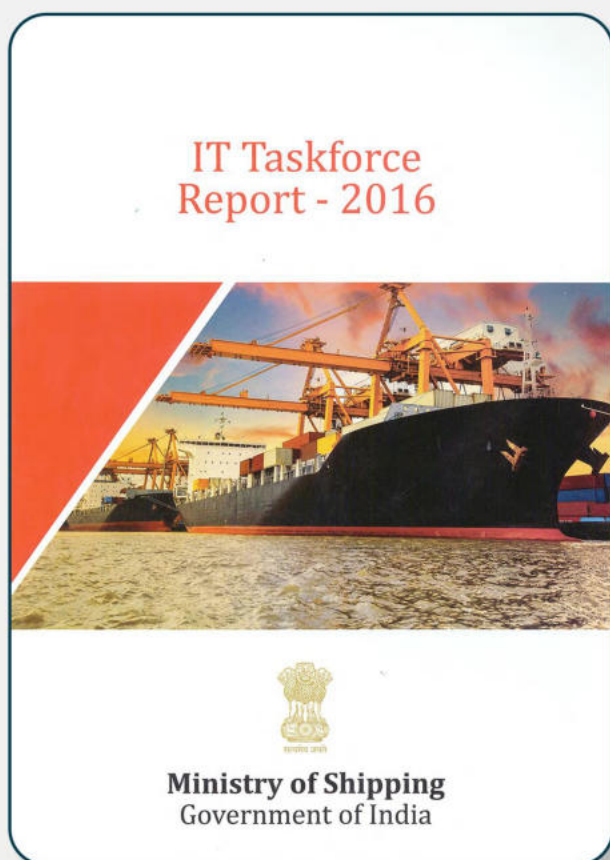
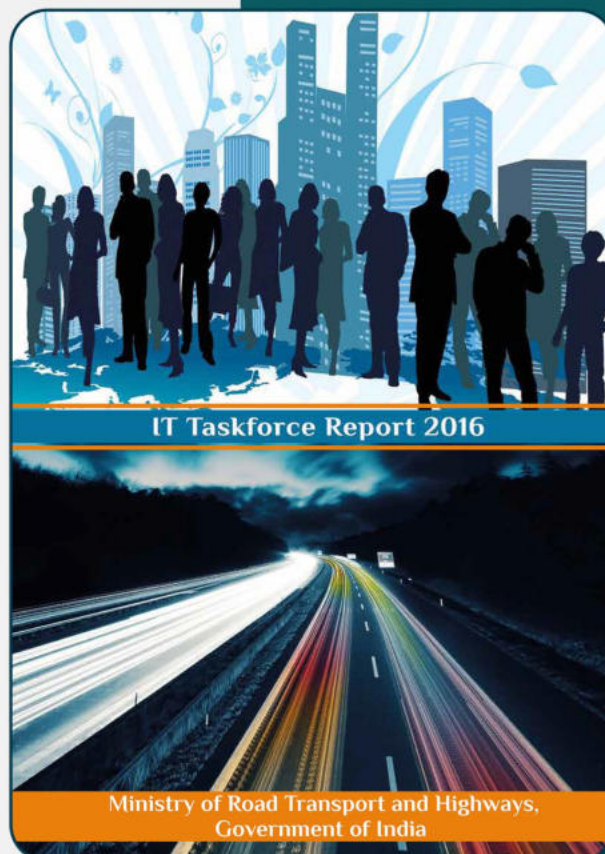
GLIMPSES





Publications Reports & Books

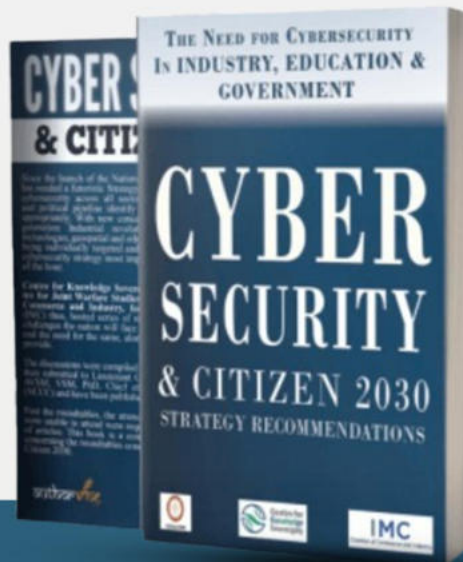
Taskforce Reports



Publications



Data Sovereignty: The Pursuit of Supremacy



Cyber Security & Citizen 2030 : Strategy Recommendations

Recommendations

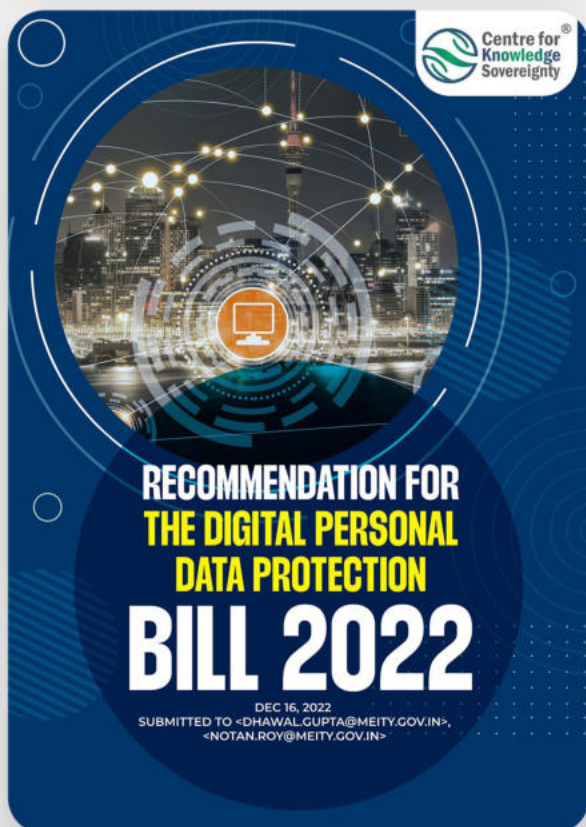


RECOMMENDATIONS FOR NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020)

Hosted By:



IMC
Chamber of Commerce and Industry



RECOMMENDATION FOR THE DIGITAL PERSONAL DATA PROTECTION BILL 2022

DEC 16, 2022
SUBMITTED TO <DHAWAL.GUPTA@MEITY.GOV.IN>
<NOTAN.ROY@MEITY.GOV.IN>



Centre for
Knowledge
Sovereignty

STRATEGY to DEAL WITH NATIONAL SECURITY THREAT EMANATING FROM SOCIAL MEDIA

www.cksindia.in

Reports



Leveraging **Information Technology** for
Economy, Transparency, Speed, Inclusion,
Scalability and Robust solutions in
Transportation

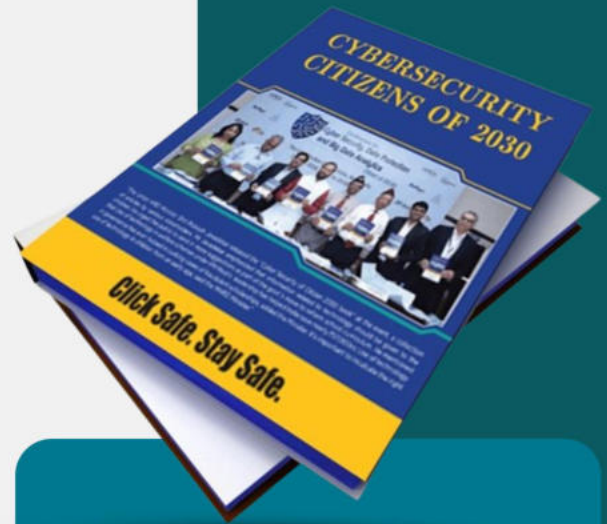
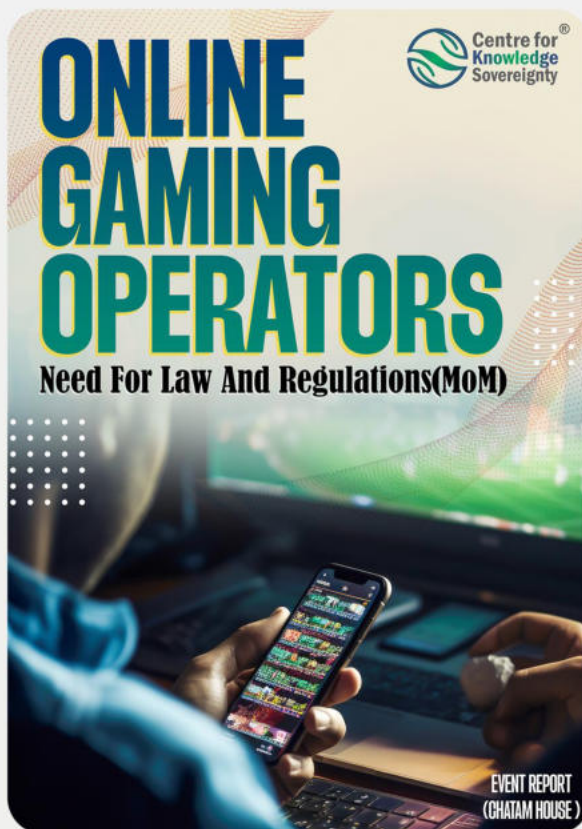
By
Vinit Goenka



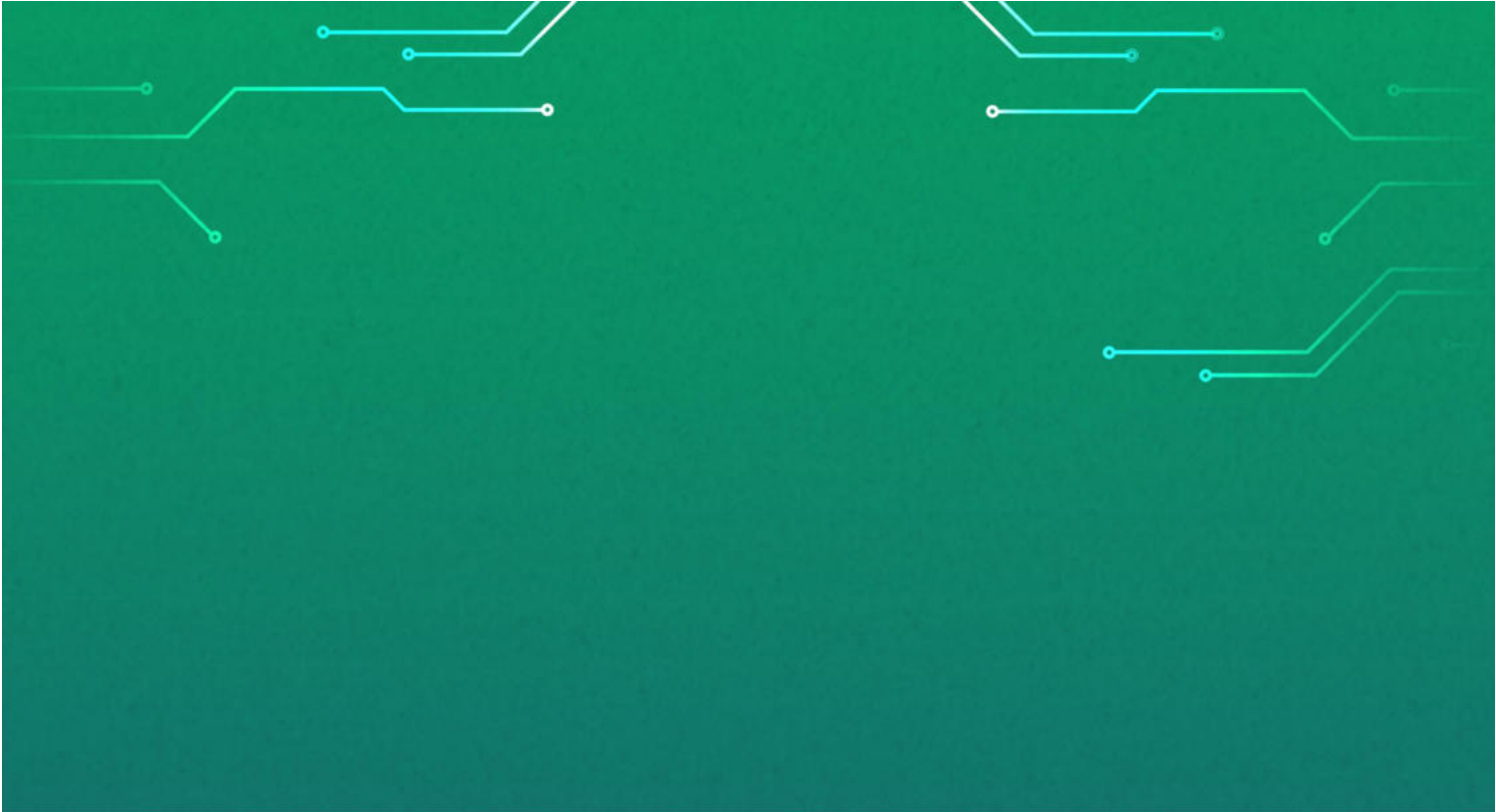
#ITForParivahan



Reports



Cybersecurity Citizens of 2030

The top header features a dark green background with light green circuit-like lines and nodes. These lines are composed of horizontal, vertical, and diagonal segments, with small circles at the endpoints, resembling a stylized electronic circuit.

Flagship Initiatives

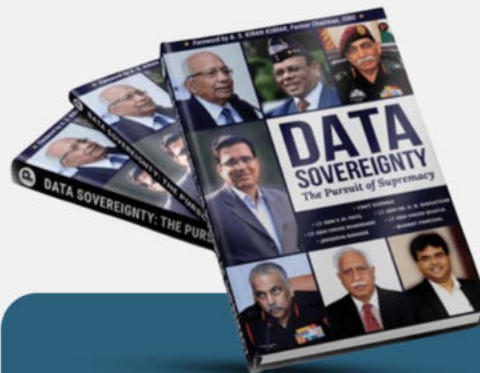
The bottom footer has a dark blue background with light blue circuit-like lines and nodes. Similar to the top header, these lines are made of horizontal, vertical, and diagonal segments with small circles at the ends, creating a symmetrical design with the top section.

Flagship Initiatives

Data Sovereignty



Inauguration at Bombay Stock Exchange, Mumbai by Former Chairman of ISRO and Vikram Sarabhai Professor Shri A S Kiran Kumar and other dignitaries.



Book Release ceremony
Data Sovereignty: The Pursuit of Supremacy



Inauguration at Constitution Club of India, New Delhi by then Organising Secretary of ABVP and current Akhil Bharatiya Prachar Pramukh, RSS Shri Sunil Ambekar ji and other dignitaries.

Flagship Initiatives

Master Mentors Geo-enabling Indian Scholars - [MMGEIS]

Master Mentors Geo-enabling Indian Scholars (MMGEIS), an online program aims to inculcate geospatial thinking and develop a research-oriented mindset amongst students who will form the future workforce of the country. The program will be open to students from 6th grade to undergraduate and will be delivered in a completely virtual mode over 5 months to provide them with much-needed exposure about what goes behind the common apps that we use to navigate our way to someplace or hail a cab or order food or other stuff from our mobile devices, or how GIS and remote sensing is playing a role in smart cities, utilities, transportation, disaster management, sustainable development etc. It is about kindling geospatial thinking which will become foundation for them to use the geospatial approach in which ever career they adopt.

ABOUT THE PROGRAM

Isaac Newton's famous words, "If i have seen further, it is by standing on the shoulders of giants," underscore the profound impact of mentors. The significance of finding excellent mentors cannot be overstated, especially for students on the cusp of pivotal life decisions. Proper guidance becomes instrumental in shaping their paths and propelling them to greater heights. The Master Mentor's Geo-enabling Indian Scholars (MMGEIS) program presents a unique opportunity for students to delve into geospatial technology and be mentored by experts in the field A joint initiative of the Centre for knowledge Sovereignty and Esri India, MMGEIS is a "not-for-profit" endeavour designed to inculcate thinking of Geospatial-innovation amongst indian scholars who will form the future workforce of India. This program is aimed at students from 6th grade to undergraduate levels and provides them a foundation on which they can develop ideas to discover new technologies ami methods in geospatial arena. The program will tap pan-India talent through a competitive process. It will bridge the gap between academia and industry access and collaborate to create a best-in-class ecosystem for geospatial innovation and Intellectual property development which will contribute towards our goal of becoming a developed nation by the year 2047

OBJECTIVE

Create awareness on the importance of "geospatial thinking" and "geospatial skills" at college/school level.
Encourage educational institutions to incorporate "geospatial thinking" and strengthen "geospatial skills" in their pedagogy and curriculum. Highlight the strategic value of geospatial in economic, social, and environmental spheres.
Strengthen geospatial learning, research, and knowledge towards creating intellectual property.

ELIGIBILITY

High School Students

Senior School Students

Undergraduate Students

No prior experience required-just a curiosity to explore, learn and problem-solving attitude !

WHY ATTEND THE PROGRAM?

Vision Talks and Interaction with Master Mentors

One-on-One Mentoring by Experts

Engaging Lessons

Interactive Activities

Spatial Thinking in Action

Knowledge Towards Creating Intellectual Property



PRIZES & REWARDS

- Certificate of Achievement
- Letter of Recommendation (LoR)
- ArcGIS Online Software (21 days)

MASTER MENTORS & BOARD MEMBERS



A.S. Kiran Kumar

Member, Space Commission &
Fmr. Chairman, ISRO



Dr. K. J. Ramesh

Advisor Regional Integrated Multi-Hazard
Early Warning System (RIMES) &
Fmr. Director General, India
Meteorological Department (IMD)



Lt. Gen. Girish Kumar, VSM (Retd.)

Advisor, Government of
Haryana and Fmr. Surveyor General of
India

BOARD MEMBERS



Vinit Goenka

Secretary
Centre for Knowledge Sovereignty



Agendra kumar

Managing Director
Esri India

ADVISORY BOARD MEMBERS

Lt. Gen. Vinod G. Khandare, PVSM, AVSM, SM (Retd.)
Fmr. Principal Advisor, Ministry of Defence, GOI
Fmr. Military Advisor NSCS, Fmr. DG Defence
Intelligence Agency.

Dr. Mrutyunjay Mohapatra
Director General
India Meteorological Department

Dr. Prakash Chauhan
Director, National Remote Sensing Centre (NRSC)

Dr. Arun Kumar Sarma
Director General, Northeast Centre for Technology
Application and Reach (NECTAR)

Dr. Raj Kumar Khatri, IAS
Co-ordinator for World Bank Project on
Land Policies (Karnataka State)

Rajesh Chandra Mathur
Senior Director - Strategy, Esri India

Lt. Gen. PJS Pannu PVSM AVSM, VSM(Retd.)
Fmr. Deputy Chief, Indian Integrated Defence Staff
(Operations)

Dr. Sultan Singh
Head GIS Division, GDMA

Dr. D. Vasudevan
Senior Consultant (Information Systems),
NAFED New Delhi

V Uday Kumar
DDG, National Informatics Centre

Dr. Sameer Saran
DGM RC North - RRSC, ISRO

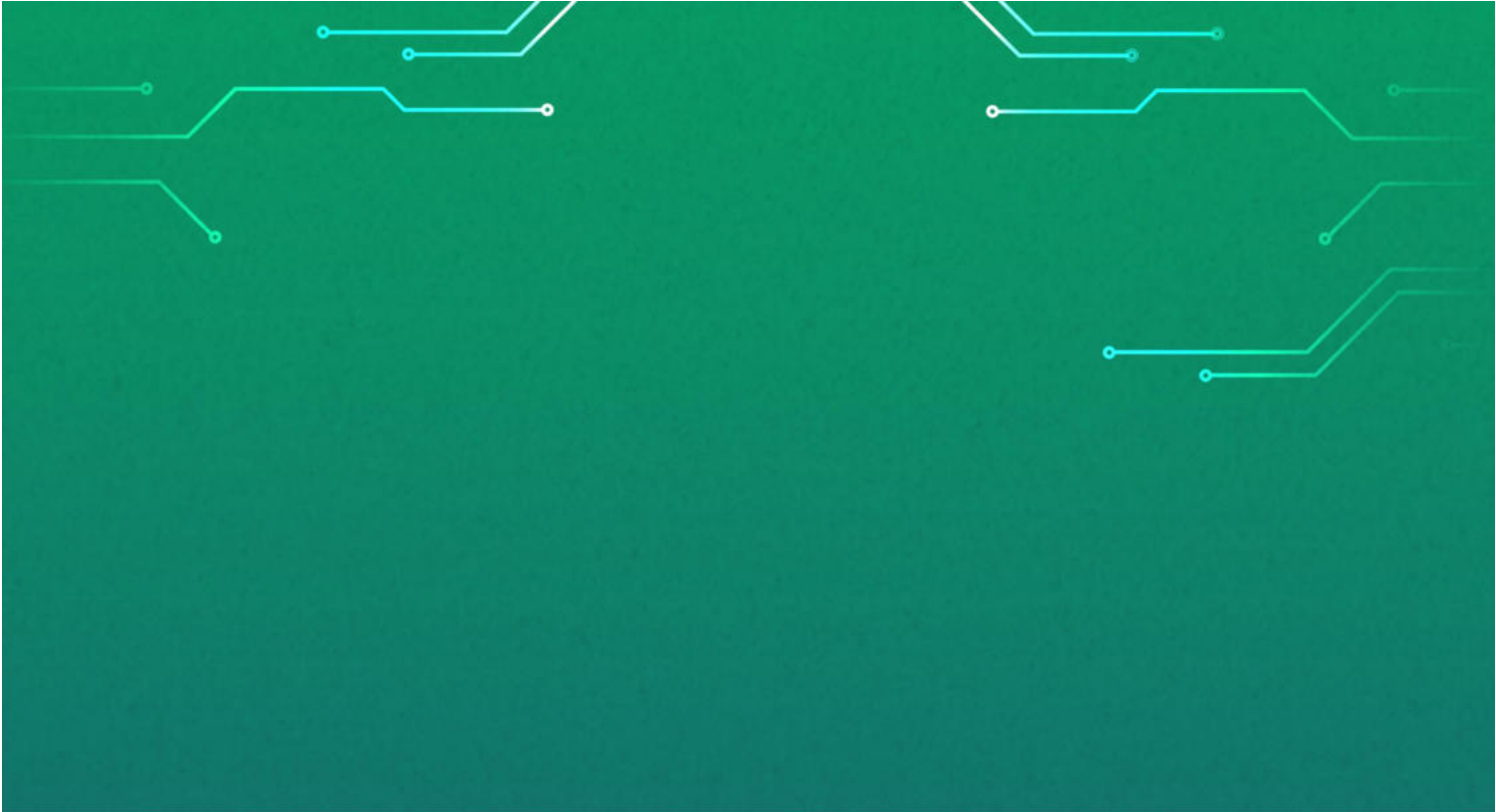
Vishnu Chandra
Advisor, Ministry of Panchayati Raj

Ravindra Kumar
Chief Scientist & Head ILT. CRRRI

Dr. Shikha Dixit
Deputy Director (Environmental Health & Geospatial
Science), INCLEN Trust, New Delhi

Pawan K Jushi PhD
Professor School of Environmental Sciences
(SES), JNU

Prof. Dheeraj Kumar
Dy. Director & Project Director (Mining Technology
Innovation Hub (TEXMIN)), IIT (ISM)



Thus Spake Generals



THUS SPAKE GENERALS

THUS SPAKE GENERALS means "Experts Speak", is a platform for high-level discussions and presentations by experts, leaders, and scholars on military, geopolitical, strategic, and knowledge-related topics.

Over the past few years, CKS is privileged to host on its platform, several discussions, round tables in person and since Covid19, CKS has initiated Virtual discussions as well. **#THUSSPAKEGENERALS** is among the flagship programs which has completed **Thirty Talks**.

We had the privilege of hosting strategists and thought leaders on our platform such as Lt Gen Dr D B Shekatkar, Lt Gen P R Shankar, Lt Gen S Kulkarni, Lt Gen Ata Hasnain, Vice Admiral Sekhar Sinha, Air Marshal SS Soman. AVM Arjun Subramaniam, Air Marshal Anil Khosla, Lt Gen D S Hooda, Lt Gen Z U Shah, Vice Admiral Anil Chopra, Lt Gen Rakesh Sharma, Rear Admiral Sudarshan Shrikhande, Air Marshal D Choudhary, Ambassador Ashok Sajjanhar, Lt Gen Shokin, Lt Gen Vinod Bhatia, Lt Gen Vinod Khandare, Lt Gen Satish Dua and many more.

PROGRAM MODERATORS

1 **AVM PRANAY SINHA**

2 **UMA SUDHINDRA**

3 **DR. DEEPA PRAKASH**

4 **SUMITRA V GOENKA**

5 **DR. NAGARATHNA A.**

6 **BIPINDRA NC**



THUS SPAKE GENERALS

(OUR SPEAKERS)



WATCH MORE DETAILS ON YOUTUBE CHANNEL



CKSINDIA

About CKS

Formed in the Year 2011, The Centre for Knowledge Sovereignty (**CKS**) is a leading autonomous, non-partisan public policy think-tank focusing on technology's impact on **data, security, and policymaking**. CKS is dedicated to **promoting and protecting** the rights of Indian citizens over their 'Knowledge' and 'Data'. Its core mission is to ensure that indigenous and local knowledge systems are preserved, respected and enhanced that data sovereignty—the right of communities to control their own 'Knowledge' and 'Data' is upheld.

At CKS, we have a firm belief in forming a sovereign future for India, we visualize India as a forerunner in creating impact through policymaking and heralding as a prominent voice for the discourse pertaining to disruptive technologies, and technological integration. We achieve this by conducting in-depth research and providing policy solutions across inter-sectoral fields, while pioneering technology and its extensive connotations.

We are empowering India's future through research and policy intervention to edifice a sovereign and sustainable digital age.

Our Value Lies in: **Shaping the Knowledge Landscape: For a Sovereign Future.**

14+
Years of Existence

40,000+
Copies of Book
"Data Sovereignty Pursuit of
Supremacy" in circulation

1M+

Students Reached through Programs
like MMGEIS, CS 2030, Grand Guru etc.

500+

Roundtable Discussions, Conferences, Policy
Consultations, Academic Forums Events etc.

Vision

Centre for Knowledge Sovereignty strives to be the region's intellectual hub and thought leader for research, analysis and advocacy on impacting policies, disruptive technologies and bring new perspectives to the policy makers.

Mission

Centre for Knowledge Sovereignty will promote sustainable and pragmatic policy initiatives collaboratively to influence the stakeholders, drive change and provide better understanding of global trend and their consequences for society, economy and national security.



 secretariat@cksindia.in



 cksindia.org



 [cksindia](https://www.youtube.com/cksindia)



 [cksindia](https://www.linkedin.com/company/cksindia)