India’s Digital Public Infrastructure

This editorial is based on “ Shock-proof state: On an outage and a democratic digital infrastructure” which was published in The Hindu on 22/07/2024. The article highlights the widespread impact of a software glitch on various services and emphasizes the need for robust failsafes and emergency protocols. It calls for a 'Digital India' initiative to ensure resilient digital infrastructure that addresses technological interconnections and societal inequalities.

For Prelims: Digital public infrastructure, Digital India, Unified Payments Interface, Aadhaar Ecosystem, Open Network for Digital Commerce, Account Aggregator Framework, Ayushman Bharat Digital Mission, Ayushman Bharat Health Account, eSanjeevani, Digital India BHASHINI , Digital Rupee, India Stack, DigiLocker, Digital Personal Data Protection Act, 2023.

For Mains: Major Challenges Related to India’s Digital Public Infrastructure, Measures to Enhance the Resilience of India’s Digital Public Infrastructure.

India positioned **digital public infrastructure** as a key pillar of its **G20 presidency,** promoting its adoption globally as a model for inclusive development. The country has made significant strides in developing its **digital public infrastructure.** However, the global software glitch on **19th July 2024** exposed **vulnerabilities in interconnected systems across critical sectors**, highlighting the need for a more comprehensive approach to digital infrastructure.

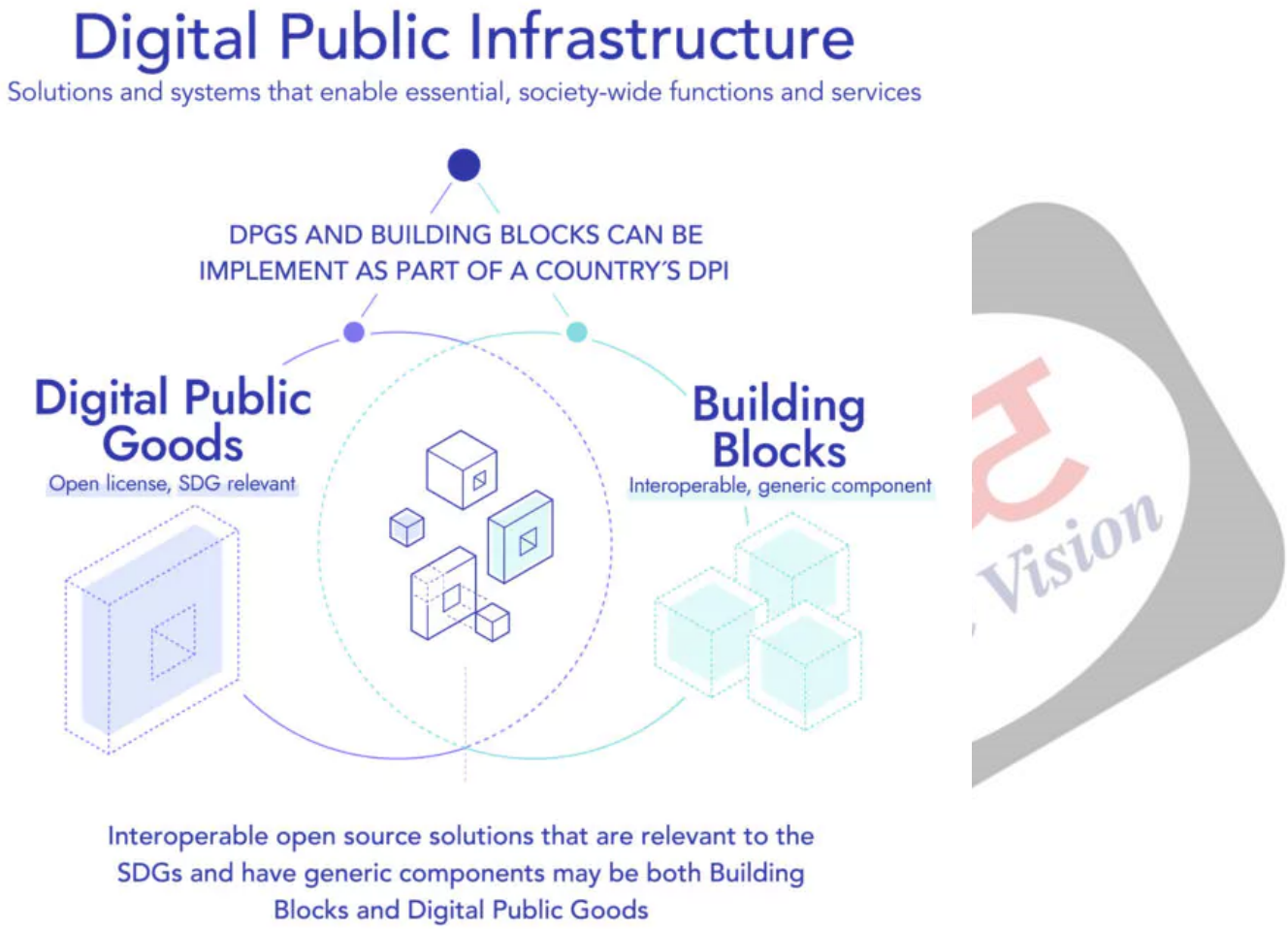
The '**Digital India**' **initiative** must evolve to address not only technological advancement but also **digital privacy, data sovereignty, and socio-economic disparities** affecting technology adoption. India needs to work diligently in this regard, focusing on creating **shock-proof digital infrastructure** that maintains essential services, supports informal economies, and builds public trust through open-source solutions and integrity testing.

What is Digital Public Infrastructure?

- **Digital Public Infrastructure (DPI)** refers to the foundational digital systems and services provided by the government or public sector to support and enhance the functioning of a digital economy and society. It includes:
    - **Digital Identity Systems:** Platforms for verifying and managing individuals' identities online, such as Aadhaar in India.
    - **Digital Payment Systems:** Infrastructure that supports secure financial transactions, including **digital wallets, payment gateways, and banking platforms.**
    - **Public Digital Services:** Online services provided by the government, such as **e-governance portals, public health information, and digital education platforms.**

- **Data Infrastructure:** Systems for storing, managing, and sharing data securely, ensuring data sovereignty and privacy.
- **Cybersecurity Frameworks:** Measures and protocols to protect digital assets and personal information from cyber threats.
- **Broadband and Connectivity:** Infrastructure ensuring widespread and equitable access to high-speed internet across regions.

//



What are the Key Developments in India's Digital Public Infrastructure?

- **Unified Payments Interface (UPI):** UPI has revolutionized digital payments in India, showing exponential growth since its inception.
  - UPI transactions have grown from 92 crore in FY 2017-18 to **8,375 crore in FY 2022-23.**
  - The system has expanded internationally, with countries like **UAE, Singapore, and France** adopting or considering UPI.
  - Recent developments include the **integration of UPI with credit cards and the launch of UPI Lite** for offline transactions.
  - These advancements have not only enhanced financial inclusion but also positioned India as a leader in digital payments globally.
- **Aadhaar Ecosystem:** Aadhaar, India's biometric identification system, has become the backbone of many government and private sector services.
  - With over **1.3 billion enrollments,** it's the **world's largest biometric ID system**.
  - The integration of Aadhaar with DigiLocker has enabled secure storage and sharing of documents.

    - This ecosystem has significantly reduced fraud in welfare distribution and streamlined KYC processes across sectors.
- **Open Network for Digital Commerce (ONDC):** ONDC represents India's ambitious attempt to democratize e-commerce.
    - Launched in the pilot phase across multiple cities, it aims to bring **30 million sellers and 10 million merchants online**.
    - By creating an open network, ONDC challenges existing e-commerce monopolies and provides a level playing field for small and medium enterprises.
- **Account Aggregator Framework:** The Account Aggregator framework is transforming financial data sharing in India.
    - It enables secure, consent-based sharing of financial information across institutions.
    - As of 2023, over **1.1 billion accounts are AA-enabled** across various banks.
        - This system has particularly benefited MSMEs, with faster loan processing times and improved access to credit.
- **Digital Health Initiatives:** India's digital health ecosystem, centered around the **Ayushman Bharat Digital Mission**, is making significant strides.
    - As of December 2023, **50 crore individuals have Ayushman Bharat Health Account (ABHA)** as their unique health ID.
    - The **CoWIN platform**, initially developed for Covid-19 vaccination, has been repurposed for universal immunization programs.
    - Telemedicine consultations have surged, with platforms like **eSanjeevani** conducting over 100 million consultations.
        - These initiatives are improving healthcare access and efficiency across India.
- **Digital India BHASHINI: BHASHINI (BHASHa INterface for India)** is an AI-powered language translation platform aimed at breaking language barriers in digital communication.
    - It's being integrated into various government websites and apps, enhancing accessibility.
- **Central Bank Digital Currency (CBDC):** The **Reserve Bank of India** launched the **Digital Rupee pilot** in December 2022, marking India's entry into the CBDC space.
    - By mid-2023, over **2.2 crore transactions** have been processed since the launch of CBDC pilot.
    - This initiative aims to reduce the cost of currency management and enable more real-time, cost-effective cross-border transactions.
- **Government e-Marketplace (GeM):** GeM portal has seen a significant surge in procurement, surpassing **Rs 1.24 lakh crore** in the first quarter of 2024-25.
    - This system has achieved a **10% savings** in public procurement costs
    - GeM's success has led to its adoption by public sector enterprises and its model is being studied by other countries for replication.

Note: **India Stack**, a set of open APIs and digital public goods, continues to evolve as the backbone of India's digital infrastructure. It includes **Aadhaar for authentication, UPI for payments,** and **DigiLocker** for document verification.

- The Consent Layer, part of the **Data Empowerment and Protection Architecture (DEPA),** enables secure data sharing.

What are the Major Challenges Related to India’s Digital Public Infrastructure?

- **The Digital Divide Dilemma:** The digital divide remains a significant challenge, with disparities in access to technology and digital literacy.
    - As of 2022, **India's internet penetration stood at about 52% (Internet in India Report 2022)**, around half the population offline.
    - Rural areas lag behind urban centers in digital adoption. For instance, **while UPI transactions are booming in cities,** many village residents still rely on cash.
    - The **National Family Health Survey 2019-21** found only **33% of Indian women** using the Internet, compared to **57% of men.**

- **Digital Literacy Lag:** While infrastructure development is crucial, equally important is enhancing digital literacy.
    - Despite initiatives like the **Pradhan Mantri Gramin Digital Saksharta Abhiyan,** a significant portion of the population remains digitally illiterate.
    - This **impacts the adoption and effective use of digital services**, from UPI to e-governance platforms.
- **Vulnerability to External Shocks:** Recently, the global IT system outage was triggered by a faulty software update from **CrowdStrike**, causing widespread disruptions across various **Windows operating system (OS) types.**
    - This overdependence created a **domino effect,** disrupting critical services across sectors.
    - The lack of robust **fail-safe mechanisms** further exacerbated the situation, highlighting the **urgent need for a more resilient digital ecosystem.**
    - With increased digitization comes heightened cybersecurity risks.
        - India businesses face over **3,000 cyberattacks per week.**
        - For instance, the recent **ransomware attack on AIIMS Delhi in 2023** exposed vulnerabilities in critical infrastructure.
- **Vernacular Issues**: In a country with 22 official languages and numerous dialects, language poses a significant barrier to digital adoption.
    - While initiatives like **BHASHINI aim to address this**, ensuring comprehensive language support across all digital platforms remains a challenge.
    - For example, many government apps and websites are still predominantly in **English or Hindi,** limiting their reach.
- **Digital Sovereignty Struggle**: India's push for data localization, as seen in draft policies, aims to ensure digital sovereignty.
    - However, this creates challenges for global tech companies and potentially impacts cross-border data flows.
    - For example, the **Reserve Bank of India's mandate for storing payment data locally** has led to compliance complexities for international payment providers.
    - Also, **Digital Personal Data Protection Act, 2023** allows transfer of personal data outside India, **except to countries notified by the central government.**
        - This mechanism may **not ensure adequate evaluation of data protection standards** in the countries where transfer of personal data is allowed.
- **Personal Data Privacy Paradox:** As digital services expand, concerns about data privacy and security intensify.
    - The provisions of the **Digital Personal Data Protection Act, 2023**, have yet to be fully implemented.
    - Incidents like the **Aadhaar data breaches reported in 2018** have raised public concerns.

What Steps can be Taken to Enhance the Resilience of India’s Digital Public Infrastructure?

- **Enhanced Cybersecurity Measures:** India should significantly increase its cybersecurity budget allocation, to reflect the growing importance of digital security.
    - **Mandatory cybersecurity audits** for all critical infrastructure sectors would help identify vulnerabilities and strengthen defenses.
    - Implementation of a **robust national cyber incident response plan,** complete with regular drills, would enhance India's preparedness to handle large-scale cyber attacks.
- **Interoperability Standards:** The development and enforcement of national interoperability standards for all digital services would ensure seamless integration and data exchange across platforms.
    - An **Open API policy for government services like Maya OS for defense** should be created to encourage innovation and enable third-party developers to build on existing infrastructure.
    - Establishing a **regulatory sandbox for testing interoperability of financial services** would promote innovation while ensuring security and compliance.
    - The adoption of the **IndEA (India Enterprise Architecture) framework** across sectors would provide a common ground for digital transformation.

- **Inclusive Digital Literacy Programs:** India should launch a nationwide "**Digital Saksharta Abhiyan 2.0**" focused on **practical digital skills,** partnering with NGOs and tech companies to reach remote areas.
    - The initiative should introduce **digital literacy modules in school curricula** from the secondary level onwards, ensuring a strong foundation for future generations.
    - **Targeted programs for women, the elderly, and marginalized communities** should be developed to bridge the digital divide.
    - These efforts would collectively work towards creating a digitally empowered society, enabling all citizens to participate in and benefit from India's digital economy.
- **Cyber Security Board:** Establish a Cyber Security Board in India, including both **government and private sector members**, with the power to analyze significant cyber incidents and recommend improvements.
    - Implement a **zero-trust architecture,** enforce a standardized incident response playbook, and urgently modernize state networks and response policies.
- **Agile Regulatory Framework:** India should establish a multi-stakeholder **Digital Economy Task Force** to enable adaptive policymaking that keeps pace with technological advancements. I
    - Developing principle-based regulations that are **technology-neutral and future-proof** would provide flexibility while maintaining necessary oversight.
- **Infrastructure Expansion:** Accelerating the BharatNet project to **connect all 600,000 villages with high-speed internet** is crucial for bridging the digital divide.
    - Promoting edge computing solutions would enable better service delivery in remote areas, reducing latency and improving user experience.
    - Developing a national strategy for **efficient 5G rollout and beyond** would ensure India stays at the forefront of wireless technology deployment.
- **Vernacular Digital Content:** Mandating **multi-lingual support for all government digital services** would ensure inclusivity and wider accessibility.
    - Developing **AI-powered real-time translation tools** for digital platforms would break down language barriers and facilitate seamless communication.
    - Implementing **voice-based interfaces for digital services** would overcome literacy barriers, making technology accessible to a broader population.
- **Green Digital Infrastructure:** Setting **energy efficiency standards for data centers and digital infrastructure** would promote sustainability in the rapidly growing tech sector.
    - Promoting the use of **renewable energy in powering digital infrastructure would reduce the carbon footprint** of India's digital economy.
    - Incentivizing **green technology adoption in the IT sector** would align India's digital growth with environmental sustainability goals.

Drishti Mains Question:

What are the critical strategies required to enhance the resilience and robustness of India's Digital Public Infrastructure in the face of technological disruptions and cyber threats?

UPSC Civil Services Examination, Previous Year Question

Q. Consider the following statements about G-20: (2023)

1. The G-20 group was originally established as a platform for the Finance Ministers and Central Bank Governors to discuss international economic and financial issues.
2. Digital public infrastructure is one of India’s G-20 priorities.

Which of the statements given above is/are correct?

(a) 1 only

(b) 2 only

(c) Both 1 and 2

(d) Neither 1 nor 2

Answer: C

Q. Consider the following statements: (2018)

1. Aadhaar card can be used as a proof of citizenship or domicile.
2. Once issued, Aadhaar number cannot be deactivated or omitted by the Issuing Authority.

Which of the statements given above is/are correct?

(a) 1 only

(b) 2 only

(c) Both 1 and 2

(d) Neither 1 nor 2

Ans: (d)

Q. In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only

(b) 1, 3 and 4 only

(c) 2 and 3 only

(d) 1, 2, 3 and 4

Ans: (b)

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only

(b) 1 and 2 only

(c) 3 only

(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**
