- **Technological Solutions**: - For the disbursement of cash for programmes like MGNREGA, all states must use the same software.
- **Strengthening Cyber-Security Measures** – The government must increase cyber security in order to ensure the cyber security of e-governance efforts.
- **Bureaucratic Opposition**: The fear of job losses should be used to overcome bureaucratic resistance by emphasising the potential benefits of e-Government.
- **Poor skill sets**: Government personnel' technical and management abilities must be strengthened by focusing on capacity building and skill development.
- **There are other roadblocks, such as digital illiteracy, bad infrastructure**, slow internet, a lack of collaboration among multiple ministries, and data security, to name a few.
  - **Digital Literacy** - Adequate awareness development for individuals living in rural regions is required so that they may participate in digital India and reap the advantages of the Internet.
- **Poor EGovernment Readiness**: India ranks low in the UN EGovernment Readiness Index due to a lack of telecommunication infrastructure and human capital.

Reforms Required

- **Rapid investment in the Bharatnet project**, which will provide internet connectivity across the country.
- **Incorporation of technology such as AI, IoT, and Blockchain into governance systems**.
- **Legislative reforms** are necessary to enable digital and e-government:
  - **Data Privacy Legislation is passed. Committee of B N SriKrishna)**
  - **The 2nd ARC recommends comprehensive e-governance laws.**
- **Prioritize cyber-security**. Revision of the national cyber-security policy is required to keep it current with threats such as cyber-espionage and cyber-warfare.
- **Focus on raising awareness and communication,** as well as developing information in vernacular languages, to make it simpler for residents, particularly in rural regions, to benefit from digital efforts.
- **Meeting the growing ambitions and needs of tech-savvy individuals**, particularly millennials, is critical.

Conclusion

The success of Digital India will be a crucial element in boosting the country's economic growth through increasing social and financial inclusion, public involvement, and governance and service delivery efficiency and accountability.

DIGITAL SOVEREIGNTY

The right of a state to manage its network in order to serve its national interests, the most essential of which are security, privacy, and commerce, is known as digital sovereignty.

- It's the power to be in charge of one's own digital destiny, including the data, hardware, and software that one uses and generates.

Digital Sovereignty's Importance

- **Eliminate technical dependency:** Identify and reduce reliance on foreign data infrastructure, combat unfair competition in digital marketplaces, and address vulnerabilities related to upcoming technologies such as 5G and AI.
- **Guaranteed data access**: **Digital sovereignty is also required for national political autonomy**, commercial innovation, and research institution freedom, since appropriate technology and data must be made available through guaranteed access.
- **Internal security and country unity**: One major fear regarding the preservation and potential exchange of personal data is that it could be exploited to pose a danger to any country's internal security.
- **digital colonialism:** Technology corporations from the United States and China may be perceived to have market domination, which might lead to new forms of hegemony and exploitation.

Digital Sovereignty's Obstacles