Prelims Exam Topics

PAIMANA PORTAL

Context

The **Ministry of Statistics and Programme Implementation (MoSPI)** continues to strengthen monitoring of Central Sector infrastructure projects through its **PAIMANA platform.**

About PAIMANA Portal

- PAIMANA (Project Assessment, Infrastructure Monitoring & Analytics for Nation-building) is a flagship initiative of the Ministry of Statistics and Programme Implementation (MoSPI).
- It functions as a centralised national repository of infrastructure projects, enabling web-generated analytical reports and enhancing data accuracy, and operational efficiency.
- It is integrated with **DPIIT's Integrated Project Monitoring Portal (IPMP/IIG-PMG) through APIs.**

Key Features of the PAIMANA Portal

- **Centralized Project Monitoring:** It serves as a centralized project monitoring system, providing a single-window interface for ministries, departments, and implementing agencies to upload, track, and review project information.
- **Real-time Dashboards:** It features real-time dashboards with drill-down capabilities, enabling users to monitor progress across sectors, states, and timelines.
- **Advanced Data Analytics:** It includes advanced data analytics, role-based user access, interactive dashboards, reporting and query modules, and review cases for identification of data gaps.
- It is mandated to monitor **Central Sector Infrastructure Projects worth ₹150 crore and above.**

11TH QUAD FOREIGN MINISTERS' MEETING

Context

- The 11th Quad Foreign Ministers' Meeting held in New Delhi focused on maritime security, energy resilience and critical mineral supply chains..

Key Decisions of the Quad FM Meeting

- **Indo-Pacific Maritime Surveillance Collaboration:** Quad members agreed to enhance maritime surveillance and information sharing across the Indo-Pacific.
    - Initiative will provide near real-time commercial maritime data to Indo-Pacific countries.

- **Energy Security Initiative:** Quad launched the **Indo-Pacific Energy Security initiative** to strengthen regional energy resilience and emergency response.
- **Critical Minerals Framework:** Quad partners agreed to deepen cooperation in mining, processing and recycling of critical minerals.
    - Quad countries aim to mobilise **$20 Billion** government and private investment for resilient critical mineral supply chains.
- **E-Waste Recycling:** Quad members will cooperate in recovery of critical minerals from electronic waste and scrap.
- **Indo-Pacific Logistics Network (IPLN):** Expanded logistics coordination for disaster relief and emergency response operations.
- **Online Scam Centres:** Quad agreed to deepen cooperation against cybercrime, trafficking and transnational organised crime.
- **Ports of the Future Partnership:** Quad announced a **pilot port infrastructure project in Fiji.**
- **Freedom of Navigation:** Quad reaffirmed commitment to freedom of navigation and unimpeded maritime commerce in the Strait of Hormuz, Red Sea and South China Sea.
- **Quad at Sea Mission:** India will host the next Coast Guard-level Quad maritime exercise.

INDIA–U.S. CRITICAL MINERALS FRAMEWORK

Context

- India and the United States signed the India–U.S. Critical Minerals Framework during the 11th Quad Foreign Ministers' Meeting.

About India–U.S. Critical Minerals Partnership

- **Framework Objective:** Strengthens cooperation in mining, processing, recycling and supply of critical minerals and rare earths.
    - Aims to reduce dependence on China-dominated mineral supply chains.
- **Strategic Importance:** Supports semiconductor, EV battery, AI and renewable energy industries.
- **Investment Cooperation:** Encourages public and private investments in critical mineral projects.
- **Recycling Focus:** Promotes recovery of minerals from e-waste and industrial scrap.
- **Regulatory Coordination:** Both countries aim to align regulations and standards for easier supply chain access.
- **National Security Link:** Critical minerals recognised as essential for economic and defence security.

Other India–U.S. Initiatives on Critical Minerals

Initiative	Launch/Year	Key Features
TRUST Initiative	2025	Stands for **Transforming the Relationship Utilising Strategic Technology**; launched during PM Modi's U.S. visit; focuses on critical minerals, semiconductors, AI and trusted technology supply chains.
FORGE	February 2026	**Forum on Resource Geostrategic Engagement** launched by U.S.; India partnered for cooperation on strategic mineral and resource security.
Pax Silica Initiative	February 2026	India joined U.S.-led initiative for resilient semiconductor, AI and critical-mineral supply chains.
Strategic Mineral Recovery Initiative	2025	India–U.S. initiative for recovery of lithium, cobalt and rare earth elements from industrial waste, coal ash and mining sectors.

SC INVOKES ARTICLE 142 TO PROTECT CHAMBAL FOREST GUARDS

Context

Recently, the Supreme Court invoked Article 142 of the Constitution while hearing a case related to rampant illegal sand mining in the National Chambal Gharial Sanctuary spread across Uttar Pradesh, Madhya Pradesh and Rajasthan.

Supreme Court's Key Directions

- The Court asked the three States to examine granting immunity under Section 218(3) of the Bharatiya Nagarik Suraksha Sanhita (BNSS) for bona fide actions taken by forest guards during anti-mining operations.
    - Similar protection is available to armed forces personnel operating in disturbed areas.
- The Court directed States to increase field-level forest staff, fill vacancies in forest departments within one year, improve patrolling and surveillance in mining-prone areas.
- The court directed technological surveillance via installation of CCTV cameras across protected zones, live-streaming surveillance mechanisms and real-time monitoring of illegal mining activities.

About Article 142 and "Complete Justice"

- **About**: Article 142 empowers the Supreme Court to pass any decree or order necessary for doing "complete justice" in matters before it.

- **Complete Justice:** The primary aim of this Article is to ensure that justice is served comprehensively, addressing situations where statutory provisions may fall short.
- **Discretionary Nature:** The powers under this article are discretionary, meaning the Court can choose when and how to exercise them based on the specifics of each case.

Supreme Court Judgments Involving Article 142

- **Governor of Tamil Nadu inaction on Bills case (2025):** The Supreme Court dealt with a constitutional crisis where the Governor of Tamil Nadu had indefinitely withheld assent on 10 Bills passed by the State Legislature.
    - **Significance:** The Supreme Court invoked Article 142 to ensure "complete justice" and held that the Governor's prolonged inaction was unconstitutional.
- **Shilpa Sailesh v Varun Sreenivasan (2023):** The Supreme Court ruled that it could directly grant a divorce on the grounds of "irretrievable breakdown of marriage" under Article 142.
    - **Significance:** This judgement allows the Supreme Court to bypass the usual procedural requirements set by the Hindu Marriage Act, which typically involves a cooling-off period for mutual consent divorces.
- **Chandigarh Municipal Corporation Elections (2023):** In this case the Supreme Court overturned election results and ensured electoral democracy was upheld.
    - **Significance:** This case illustrates how Article 142 can be used to rectify procedural irregularities in electoral processes.

Mains Exam Topics

VULNERABILITY OF INDIA'S CRITICAL INFRASTRUCTURE

Context

Recent studies and cyber-security reports highlighted growing vulnerabilities in India's critical infrastructure systems to cyberattacks and IoT-based disruptions.

Emerging Vulnerability to Critical Infrastructure

- **Expansion of Connected Infrastructure:** Increasing use of IoT and AI connected power grids, dams and fuel transport systems to the internet, making them easier targets for remote cyberattacks.
    - **E.g.** Smart grids, automated dams, GPS-enabled fuel logistics and automated monitoring systems
- **Weak Security in OT & ICS Systems**: Industrial Control Systems (ICS) and Operational Technology (OT) often lack strong cyber protection.
    - **E.g**. Attackers could alter water-treatment calibration and disrupt purification systems
- **Exposure of Government Systems:** Vulnerable government servers and surveillance systems increase risks of phishing, espionage and misinformation. (**E.g.**Government mail-server details and live CCTV feeds from Central View Dashboard were exposed online in 2021)
- **Critical Energy Infrastructure Risks**: Fuel and gas transportation systems increasingly depend on connected digital systems vulnerable to remote disruption.
    - **E.g**. GPS tracking and OTP-based fuel tanker e-lock systems now critical control points
- **Imported IoT Device Risks**: Use of unverified imported sensors, cameras and communication devices may create hidden backdoor vulnerabilities. (**E.g**. Chinese-made GPS-enabled locks used in fuel supply chains)
- **Inadequate Certification Mechanisms:** Security certification exists only for limited device categories.
    - **E.g.** STQC certification available mainly for cameras, not all IoT devices)
- **Human Error & Poor Cyber Hygiene:** Weak passwords, outdated software and poor configuration practices remain major causes of breaches.
    - E.g. India recorded 13 critical installations using default credentials(factory-set usernames and passwords assigned to devices) — highest among 20 countries studied)
- **Interconnected Infrastructure Risks**: Failure in one sector can trigger cascading disruption across power, banking, telecom and transport networks.

- **National Security Threat:** Cyberattacks on critical infrastructure can affect economic stability, governance and sovereignty. (**E.g**. 2020 Mumbai power outage allegedly linked to Chinese malware targeting India's power grid)

Government Measures to Safeguard Critical Infrastructure

- **CERT-In:** Indian Computer Emergency Response Team acts as the national nodal agency for cyber-security incident response.
- **NCIIPC:** National Critical Information Infrastructure Protection Centre protects strategic sectors like power, banking, telecom and transport.
- **National Cyber Security Policy**: Provides framework for securing cyberspace and critical digital infrastructure.
- **Cyber Surakshit Bharat Initiative:** Enhances cyber-security awareness and capacity-building across government departments.
- **STQC Certification:** Security testing and certification introduced for surveillance cameras and electronic devices.
- **Trusted Telecom & Electronics Push:** Government promoting indigenous and trusted digital infrastructure under Atmanirbhar Bharat.

Structural Issues Despite Government Measures

- **Weak Policy Enforcement:** Existing IoT and cyber-security guidelines are often poorly implemented across PSUs and local agencies.
- **Template-Based Procurement:** Procurement systems prioritise compliance paperwork rather than deep security audits and design verification.
- **Limited Indigenous Ecosystem:** Dependence on imported hardware and components increases strategic vulnerability.
- **Fragmented Institutional Coordination:** Multiple agencies handle cyber-security with limited integrated response mechanisms.
- **Lack of Skilled Workforce:** India faces shortage of specialised cyber-security and industrial cyber-defence professionals.
- **Slow Certification Processes:** Security certification for IoT devices remains limited, lengthy and unevenly enforced.

Way Forward

- **Strengthen OT & IoT Security:** Extend cyber-security standards beyond IT systems to industrial control and connected infrastructure.

- **Mandatory Security Audits:** Conduct periodic vulnerability assessments and red-team testing for critical infrastructure.
- **Promote Indigenous Technologies:** Reduce dependence on unverified imported hardware in sensitive sectors.
- **Integrated National Cyber Framework:** Improve coordination between government, PSUs and private operators for real-time response.
- **AI-Based Threat Detection:** Deploy AI-enabled monitoring systems for early anomaly and intrusion detection.
- **Build Skilled Workforce:** Expand specialised training in SCADA, industrial cyber-security and digital forensics.

ANTI-DEFECTION LAW

Context

Recent political developments in the Rajya Sabha and the Tamil Nadu Legislative Assembly have once again brought India's anti-defection framework into national focus.

Recent defection disputes

- **Merger and Defection in Rajya Sabha**: Seven Rajya Sabha MPs of the Aam Aadmi Party reportedly invoked the "merger" provision under the Tenth Schedule to join the ruling party, raising constitutional questions on whether legislators alone can merge with another party without the consent of the original political party.
- **Resignation and Disqualification Issue in Tamil Nadu:** The resignation of AIADMK MLAs in Tamil Nadu, who later joined the ruling Tamilaga Vettri Kazhagam, revived debate over whether resignation can nullify pending disqualification proceedings under the Anti-Defection Law.

About the Tenth Schedule

Added through the **52nd Constitutional Amendment in 1985**, the Tenth Schedule contains various features:

Grounds for Disqualification

- A legislator can lose their seat if they voluntarily relinquish membership of their political party.
- A member who votes or abstains in the House against the party's whip can be disqualified.
- Independent legislators are disqualified if they join any political party after an election.
- Nominated members will lose their seat if they join a party after six months from the date on which they enter the legislature.

Exceptions in the Law

- A political party may legally merge with another if two-thirds of its legislators support the merger. (Paragraph 4 of the law)
- Both the group that merges and the group that stays back are protected from disqualification.
- The law also exempts presiding officers (Speaker, Chairman, Deputy Chairman) from disqualification if they resign from their party during their tenure or rejoin after their term ends ensuring neutrality and dignity of the office.
- Anti-defection provisions do not apply to votes in presidential elections.

Authority to Disqualify

- The Speaker or Chairman of the House is responsible for ruling on disqualification petitions.
- If the allegation is against the presiding officer themselves, another member chosen by the House takes the decision.

Supreme Court's case laws

- **Subhash Desai vs Principal Secretary, Governor of Maharashtra (2023):** The Supreme Court clarified that:
    - Legislature parties cannot function independently of their parent political parties
    - Elected representatives continue to remain politically connected to the original party even after elections
- **Shrimanth Balasaheb Patel Case (2019):** During the Karnataka political crisis, several MLAs resigned amid allegations of defection intended to destabilise the government.
    - **Limited Role of the Speaker:** The Court held that while considering resignation letters, the Speaker can examine only whether the resignation is voluntary and genuine and the Speaker cannot investigate political motives or external considerations.
    - **Resignation Does Not Erase Defection:** The "taint" of disqualification does not disappear merely because a legislator resigns before adjudication. Defection relates back to the date on which the act of disqualification occurred.

Importance of the Anti-Defection Framework

- **Political Stability:** Frequent defections weaken governments, disrupt administration, and create instability in coalition politics.
    - Eg: Aaya Ram, Gaya Ram
- **Electoral Mandates:** Voters elect candidates largely based on party ideology, leadership, and manifesto commitments. Defections can therefore distort public mandate.

- **Democratic Accountability**: Political parties remain central to parliamentary democracy. Weakening party discipline may encourage political opportunism and instability.
- **Maintaining Public Trust:** Unethical defections create public cynicism regarding democratic institutions and legislative morality.

Challenges in the Present Framework

- **Excessive Party Control:** Strict enforcement of party whip may reduce independent thinking among legislators and weaken deliberative democracy.
- **Delay in Decision-Making:** Speakers often delay anti-defection decisions for political reasons, affecting neutrality and fairness.
- **Questions on Speaker's Neutrality:** Since the Speaker usually belongs to a political party, concerns arise regarding impartiality in adjudicating disqualification cases.
- **Legal Ambiguity**: The Constitution does not clearly define:
    - Whether legislature parties can independently merge
    - Whether resignation ends Speaker's jurisdiction

Conclusion

The Anti-Defection Law was intended not merely to regulate political behaviour, but to preserve the integrity of representative democracy itself. Judicial clarity, institutional neutrality, and procedural reforms will be essential to ensure that constitutional morality remains stronger than political conveniences.