6. Digital Arrests- Polity

Supreme Court gives CBI free hand to stop 'digital arrest' scams. To combat the rising menace of "Digital Arrest" scams where fraudsters impersonate law enforcement to extort money, the Supreme Court has ordered a pan-India CBI probe, mandating States to grant consent under the DSPE Act to dismantle these cross-border syndicates.

The Supreme Court Intervention

The Directive- The Supreme Court of India has directed the Central Bureau of Investigation (CBI) to lead a comprehensive pan-India probe into the rising cases of 'digital arrest' scams.

Objective- To centralize the investigation of these complex, cross-border cybercrimes that often overwhelm local state police forces.

Understanding 'Digital Arrest'

Definition- It is a sophisticated cyber scam where fraudsters impersonate law enforcement officials (Police, CBI, Customs, ED) to extort money.

Core Mechanism- The scam relies on psychological coercion, instilling intense fear and panic in the victim to force a payment.

Modus Operandi

1. **Initial Contact-** Begins with a seemingly harmless call regarding a parcel delivery issue or KYC verification.
2. **Escalation-** Quickly escalates to false claims of illegal goods found in the parcel or money laundering links.
3. **The "Arrest"-** Victims are kept on a video call (sometimes for days), told they are under "digital surveillance," and threatened with physical arrest, frozen bank accounts, or passport cancellation unless they transfer money for "verification."

Reasons Behind the Rise of these Scams

Psychological Manipulation- fraudsters exploit the general public's confidence and fear of law enforcement agencies. The term "Arrest" triggers immediate panic, bypassing rational thinking.

Digital Vulnerability

Easy Access- Fraudsters have easy access to SIM cards and spoofed IDs (making calls appear to come from official numbers).

Mule Accounts- Widespread availability of "mule bank accounts" (rented accounts) to launder the stolen money quickly.

Vulnerable Target Groups

Elderly Citizens- Often less tech-savvy and more fearful of legal trouble.

Women & Professionals- Targeted despite being educated, as they are often unfamiliar with specific cybercrime safeguards.

Organized Syndicates- Operations are not isolated but run by organized networks. "Jamtara-style" Evolution- These syndicates now have international links, operating across borders to evade local jurisdiction.

Supreme Court's Recent Directions

The Court outlined a multi-pronged approach to tackle this menace-

Empowering the CBI-

Full Authority- The CBI is granted authority to investigate not just the scammers but also bankers involved in facilitating mule accounts.

Coordination- CBI must coordinate with State police, Interpol, and online intermediaries (social media/tech platforms).

State Cooperation (Legal Mandate)-

Section 6 of DSPE Act- States were ordered to grant consent to the CBI under Section 6 of the Delhi **Special Police Establishment Act**. This removes the bureaucratic hurdle of seeking state-by-state permission for this specific probe.

Regional Integration- Regional cybercrime coordination centers are mandated to link directly with the

Indian Cybercrime Coordination Centre (I4C).
Accountability for Telecom Operators-
Negligence highlighted- The Court criticized telcos for negligent SIM issuance verification processes.
Corrective Action- The Department of Telecommunications (DoT) has been tasked with proposing measures to prevent SIM misuse.
Focus Areas- Urgent action is required not just for digital arrests but also for investment scams and part-time job frauds.

Government Steps & Institutional Framework

Institution/Initiative	Key Role & Function
Indian Cyber Crime Coordination Centre (I4C)	Established by the Ministry of Home Affairs (MHA). It coordinates national efforts to combat cybercrime and provides prevention resources.
National Cyber Crime Reporting Portal	A dedicated portal for the public to report cybercrimes. It places a special focus on cases involving women and children for swift action.
Financial Cyber Fraud Reporting System	Launched in 2021. Allows immediate reporting of financial frauds to block flow of funds. Impact- Saved over ₹3431 Crore across 9.94 lakh complaints.
Cyber Forensic Labs	Includes the National Cyber Forensic Laboratory (Delhi) and Evidence Lab (Hyderabad). Significantly improved police capability to analyze digital evidence.

Way Ahead

Nature of Threat- Digital arrests are a hybrid threat combining cyber fraud with psychological warfare.
Technological Safeguards- Implementation of AI-driven fraud detection systems by banks and telcos. Stricter, more secure SIM issuance protocols.
Legal & Policy Reforms- Need for reforms specifically addressing impersonation of government officials in the digital space. Enhanced International Cooperation to tackle cross-border syndicates.
Community Vigilance
Public Awareness Campaigns- Educating citizens that police do not conduct arrests via video calls. Encouraging citizens to report suspicious activity immediately to preserve evidence.
Source- https-//www.thehindu.com/news/national/supreme-court-entrusts-cbi-with-pan-india-probe-into-digital-arrest-cases/article70344884.ece