7. Digital Arrest- Polity

Supreme Court gives CBI free hand to stop 'digital arrest' scams. The Supreme Court has ordered an "extraordinary" pan-India CBI probe into 'Digital Arrest' scams, directing states to accord consent under the DSPE Act to tackle transnational syndicates that have caused losses over ₹3,000 crore. The directive also mandates strict SIM verification by telecom operators and collaboration between the CBI, RBI, and I4C to dismantle banking and digital infrastructure used by fraudsters.

Supreme Court Directions on CBI Probe

Pan-India Investigation Authority- The Supreme Court has authorised the Central Bureau of Investigation (CBI) to launch a comprehensive, pan-India probe.

Free Hand-The agency has been given a "free hand" to examine complex networks, specifically focusing on mule account networks and banking-linked corruption.

Exceptional Circumstance (State Consent)- Typically, the CBI requires state consent to investigate within a state's jurisdiction. However, the Court termed this an extraordinary step due to compelling circumstances.

Directive to States- 13 States (including Bihar, Tamil Nadu, Karnataka, Kerala) have been explicitly directed to accord consent under Section 6 of the Delhi Special Police Establishment Act (DSPE Act). This consent allows the CBI to investigate offences under the Information Technology Act, 2000 within these states.

Prioritization of Cases (Stage-Wise)- The investigation will follow a specific hierarchy of priority-

1. Digital Arrest Scams (Top Priority)
2. Investment Scams
3. Job Scams

Collaborative Mechanisms-

Multi-State Teams- The CBI must identify and collaborate with state police officers and cyber specialists.

International Cooperation- Recognizing the global footprint of these scammers, the CBI is instructed to coordinate with **Interpol** to identify foreign cybercrime hubs.

Intermediary Liability- Under the IT Rules 2021 (Intermediary Guidelines & Digital Media Ethics Code), digital platforms are mandated to cooperate with the CBI and share necessary data.

Role of RBI and Banking- The Reserve Bank of India (RBI) has been asked to explain the utilization of AI/ML technologies. The focus is on detecting "layering"—the technique used to move scam money across multiple bank accounts to hide its trail.

Institutional Strengthening- All States and Union Territories must establish regional cybercrime coordination centres. These must be linked with the central Indian Cybercrime Coordination Centre (I4C).

Accountability in the Telecom Sector

Judicial Criticism- The Court criticised the "alarming and irresponsible" issuance of multiple SIM cards in the same name by telecom operators, which facilitates these crimes.

Department of Telecommunications (DoT) Action- The DoT is required to submit a proposal for stricter SIM-verification measures. These measures must be enforced rigorously by all telecom service providers

Understanding Digital Arrest Scams

Definition- A cyber-extortion scheme where fraudsters impersonate law enforcement officers. They falsely accuse victims of crimes to extort money through intimidation.

Core Mechanism- It relies on psychological coercion. Scammers claim the victim is involved in illegal activities (e.g., parcel seizure containing drugs, financial fraud, tax evasion). They use the fear of imminent arrest to force immediate payments.

Imodus Operandi

Step 1- Impersonation- Criminals initiate contact via calls or emails, posing as officials from CBI, Police, Income Tax, Customs, or RBI.

Step 2- The Digital Setup- Victims are coerced into joining video calls on WhatsApp or Skype. Scammers use a fake police-station backdrop to create an illusion of authenticity.
Step 3- The "Digital Arrest"- Fraudsters issue a fabricated **"**digital arrest warrant". Victims are forced to stay online and visible on camera for hours, mimicking police custody.
Step 4- The Threat- Accusations of money laundering, tax violation, or cybercrime are levied to create panic and urgency.
Step 5- The Extortion- Victims are instructed to "clear their name" by transferring money. Funds are sent to designated accounts often labelled as "escrow wallets" or "verification deposits."
Step 6- The Aftermath- Once the transfer is complete, the scammers go offline. This results in financial loss and potential misuse of the victim's identity documents.

Magnitude and Need for Action

Financial Impact- A government note to the Supreme Court revealed that over ₹3,000 crore has been stolen through such scams.
Target Demographic- Senior Citizens are disproportionately targeted due to their fear of authority and lack of familiarity with digital crime patterns.
Institutional Flags- CERT-In (Indian Computer Emergency Response Team) has flagged digital arrest as an emerging high-risk cyber threat, alongside deepfakes and investment scams.

Classification of Cyber Frauds (Amicus Curiae)

The Amicus Curiae classified the prevailing cyber frauds into three distinct categories aimed at defrauding citizens-

Category	**Nature of Scam**	**Key Target/Method**
Digital Arrest Scams	Impersonation, Coercion, Extortion	Uses fear of arrest/law enforcement.
Investment Scams	Financial Fraud	Uses fake trading apps and promises of high returns.
Job Scams	Employment Fraud	Fraudulent part-time work offers targeting unemployed youth.

Government Initiatives to Combat the Threat

Indian Cybercrime Coordination Centre (I4C)- Operates under the Ministry of Home Affairs (MHA). Leads national efforts against cybercrime. Manages the National Cyber Crime Helpline (1930) for quick reporting and fund freezing.
National Cybercrime Reporting Portal (cybercrime.gov.in)-Allows victims to file complaints online. Facilitates real-time freezing of fraudulent transactions by connecting users to police.
Cyber Fraud Management System (CFMS)- A coordinated mechanism involving banks, payment apps, and the RBI. Enables instant freezing of suspected transactions to minimize financial loss.
Sanchar Saathi Portal (Department of Telecommunications)
Function- Tracks and blocks fraudulent mobile numbers, SIM cards, and fake caller IDs.
CEIR (Central Equipment Identity Register)- A feature within the portal to block stolen devices to prevent their use in cybercrimes.

SIM Binding Requirement

Mandate- Messaging platforms (WhatsApp, Telegram, Signal) must link their services to the SIM card used during registration.
Continuous Link- Services must remain linked to that specific SIM.
Objective- To prevent impersonation, spoofing, OTP bypass attacks, and cross-border fraud.
Source- https- //www.thehindu.com/news/national/supreme-court-entrusts-cbi-with-pan-india-probe-into-digital-arrest-cases/article70344884.ece