ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

Educational Institution Security — Bomb Threats, Cyber Hoaxes, and the Safety Deficit

INDIAN EXPRESS

16 March 2026

SUBJECTS COVERED

SOCIAL ISSUES | POLITY | SECURITY & DEFENCE

GS PAPERS

GS2 | GS3

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator •
linkedin.com/in/epicbharat

ujiyari

Educational Institution Security — Bomb Threats, Cyber Hoaxes, and the Safety Deficit

The Indian Express 16 March 2026 GS2 GS3

IE The Indian Express | MAINS RELEVANCE: GS Paper 2 GS Paper 3

INTERVIEW ANGLE

"Recurring bomb threats to schools expose gaps in India's cyber crime response, student safety protocols, and the psychology of institutional disruption. How should the government balance security with the right to education?"

WHY IN NEWS

A fresh wave of email and social media bomb threats to schools across multiple Indian cities has prompted a coordinated response from the Ministry of Home Affairs, state police, and the Department of Telecommunications — highlighting that educational institutions remain vulnerable targets for cyber-based disruption and that existing safety protocols are inadequate.

THE PATTERN OF SCHOOL BOMB THREATS

India has witnessed repeated waves of bomb threat hoaxes targeting schools since at least 2023. These threats:

- Are typically sent via **anonymous email accounts** using foreign servers (Gmail, ProtonMail etc.)
- Arrive at school principals' inboxes or are shared on parental WhatsApp groups
- Force immediate evacuation, police checks, and cancellation of the school day
- Have almost universally been hoaxes — no actual device has been found
- Cause significant **psychological trauma** to children, parents, and teachers

Scale and Pattern

- **2023 Delhi schools wave:** Hundreds of schools received threats in April–May 2023
- **2024 follow-up threats:** Multiple Delhi and NCR schools targeted again
- Similar incidents reported in Mumbai, Hyderabad, Bengaluru, and Kolkata
- Threats timed to coincide with examinations, school events, or politically sensitive days

THE CYBER ANGLE — VOIP, SPOOFING, AND ANONYMOUS EMAIL

The perpetrators exploit anonymity tools:

Method	How It Works
Anonymous email	Free email services accessible via VPN; headers traced with difficulty
IP spoofing	Masking origin IP address to appear from another country
VoIP calls	Internet-based calls from untraceable numbers
Dark web tools	Some threats linked to dark web infrastructure

India's **cyber crime reporting mechanism — Cyber Crime Portal (cybercrime.gov.in)** and the **Indian Cyber Crime Coordination Centre (I4C)** under MHA — are the primary response bodies, but attribution remains slow due to cross-border complexity.

LEGAL FRAMEWORK

Information Technology Act, 2000 (IT Act)

Section 66A (struck down by SC in Shreya Singhal v. Union of India, 2015): originally covered online messaging causing annoyance or menace

Section 66F: Cyber terrorism — using computer resources to strike terror; punishable with life imprisonment

Section 43, 66, 66B: Hacking, identity fraud — applicable in some threat cases

Indian Penal Code / Bharatiya Nyaya Sanhita (BNS)

BNS Section 351 (Criminal Intimidation): threatening person with injury

BNS Section 308 (Waging war / terrorist act provisions): false alarm of bomb may attract public mischief provisions

Explosive Substances Act, 1908: making false threats involving explosives

Challenges in Prosecution

Anonymous accounts and foreign email servers complicate evidence gathering

Mutual Legal Assistance Treaties (MLATs) needed for data from US-based companies (Google, Meta, Microsoft) — slow process (months to years)

Juveniles involved in some cases — different prosecution framework

RIGHT TO EDUCATION VS RIGHT TO SAFETY

Article 21-A of the Indian Constitution guarantees **free and compulsory education** for children aged 6–14. The **Right to Education Act, 2009 (RTE)** operationalises this.

Repeated school closures due to bomb threats directly **interrupt the right to education**, with disproportionate impact on children from lower-income families who cannot access private tutoring or make up for lost instructional time.

The conflict is between:

Security imperative: Every threat must be taken seriously until cleared

Disruption cost: Mass evacuations, psychological harm, lost learning days

GOVERNMENT RESPONSE AND MEASURES

Ministry of Home Affairs (MHA)

Issued advisories to state police to establish **Standard Operating Procedures (SOPs)** for threat response

Directed installation of **CCTV cameras** at school entry points (partially funded via Nirbhaya Fund)

I4C established Fast Response Teams for cyber crime incidents

Department of Telecommunications

Working to block VoIP numbers used for threats

Coordinating with telecom providers on caller ID authentication for institutional numbers

School Safety Infrastructure

Safe School Initiative framework recommends: perimeter security, visitor management systems, mock drills

However, implementation is uneven — private schools in urban areas have better infrastructure; government schools in rural areas have minimal security

PSYCHOLOGICAL AND SOCIAL IMPACT

Repeated evacuation drills and real threats cause **anxiety, hypervigilance, and school avoidance** in children

Teachers face dual trauma: responsible for student safety while also personally vulnerable

Parents lose trust in institutional safety, sometimes withdrawing children from school temporarily

Long-term cognitive impact: Research (APA) links school safety fears with reduced academic performance

UPSC RELEVANCE

Prelims: I4C (Indian Cyber Crime Coordination Centre), IT Act Section 66F (Cyber terrorism), Cyber Crime Portal, RTE Act 2009 (Article 21-A), MLAT.

Mains GS-2: "Repeated bomb threats to schools reflect gaps in India's cyber crime response architecture. Critically examine the legal framework and suggest institutional reforms."

Mains GS-3: "Internal security threats have evolved from physical to cyber-based disruptions. Evaluate India's preparedness to handle cyber threats to critical civilian infrastructure including educational institutions."

📌 FACTS CORNER — KNOWLEDGEPEDIA

LEGAL FRAMEWORK:

IT Act 2000, Section 66F: Cyber terrorism; punishment: imprisonment up to life

Shreya Singhal v. Union of India (2015): SC struck down IT Act Section 66A as unconstitutional

Bharatiya Nyaya Sanhita (BNS): replaced IPC from July 1, 2024

Explosive Substances Act: 1908 (colonial era); covers threats involving explosives

CYBER CRIME INFRASTRUCTURE:

I4C: Indian Cyber Crime Coordination Centre; under MHA; set up 2018

Cyber Crime Portal: cybercrime.gov.in; for online reporting

CERT-In: Computer Emergency Response Team India; under MeitY; handles cyber incidents

National Cyber Security Policy: 2013 (revision under way)

EDUCATION RIGHTS:

Article 21-A: Right to Education (86th Constitutional Amendment, 2002)

RTE Act: Right of Children to Free and Compulsory Education Act, 2009

Age coverage: 6–14 years

School safety: Nirbhaya Fund used for school CCTV in some states

MLAT AND INTERNATIONAL COOPERATION:

MLAT: Mutual Legal Assistance Treaty — for evidence sharing across borders

India has MLATs with 42+ countries including USA, UK, Russia

CLOUD Act (USA 2018): allows US courts to compel US tech firms to provide data regardless of where it's stored

OTHER RELEVANT FACTS:

India's school count: ~1.5 million schools (public + private); ~260 million enrolled students

DISE+ (Unified District Information System for Education): collects school-level data

Bomb Threat Assessment Committees: mandated by DGCA for airports; no equivalent standard for schools

NCA (National Crime Agency, UK) and FBI have dedicated school threat units — India lacks equivalent

Sources: Indian Express, MHA, NCPCR

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Published on **ujiyari.com** · Free UPSC & State PCS Current Affairs