UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

Encrypted Platforms and Digital Terrorism — The Dark Digital Ecosystem

THE HINDU

21 March 2026

SUBJECTS COVERED

SECURITY & DEFENCE SCIENCE & TECH POLITY

GS PAPERS

GS2 GS3

CURATED & WRITTEN BY

Bharat Choudhary

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

Encrypted Platforms and Digital Terrorism — The Dark Digital Ecosystem

The Hindu 21 March 2026 GS2 GS3

TH The Hindu | MAINS RELEVANCE: GS Paper 2 GS Paper 3 |

INTERVIEW ANGLE

"How should democracies balance the right to privacy with the need to intercept encrypted communications used for terrorism?"

WHY IN NEWS

The Hindu editorial examines how encrypted communication platforms have created a “dark digital ecosystem” enabling terrorism, citing the UP ATS 2026 case that revealed use of VPN-based anonymous accounts and encrypted apps like Session for terror coordination.

THE CORE PROBLEM

The editorial argues that the rapid diffusion of encrypted communication technologies has fundamentally shifted terrorism from physical networks to **covert digital ecosystems**, enabling:

- **Anonymity** — end-to-end encryption prevents interception even by law enforcement with court orders
- **Transnational connectivity** — operatives across borders coordinate in real-time without physical meetings
- **Real-time coordination** — attack planning, fund transfers, and recruitment happen on encrypted channels
- **Decentralised cells** — no central command structure needed; “lone wolf” attacks enabled by online radicalisation

THE UP ATS 2026 CASE

The **Uttar Pradesh Anti-Terrorism Squad (ATS)** uncovered a terror network in 2026 that used:

- **Session** — an open-source encrypted messaging app that requires no phone number or email to register
- **VPN-based anonymous accounts** — routing traffic through multiple countries to avoid IP tracing
- **Cryptocurrency** — for untraceable fund transfers
- **Dark web forums** — for recruitment and propaganda

This case highlighted that traditional surveillance tools (phone tapping, metadata analysis) are increasingly ineffective against operatives using privacy-first platforms.

TYPES OF ENCRYPTED PLATFORMS

Platform	Encryption Type	Key Feature
WhatsApp	End-to-end (Signal protocol)	Metadata available to company; complies with some law enforcement requests
Signal	End-to-end (Signal protocol)	Minimal metadata stored; open-source; widely considered most secure
Telegram	Optional E2E (Secret Chats only)	Regular chats are cloud-based (accessible to Telegram); Secret Chats are E2E
Session	Onion routing + E2E	No phone/email needed; decentralised; extremely hard to trace
Briar	E2E + mesh networking	Works without internet (Bluetooth/Wi-Fi); designed for activists

INDIA'S LEGAL FRAMEWORK

Existing Laws

Law	Provision	Limitation
IT Act, 2000 (Section 69)	Government can intercept/decrypt digital communications in interest of sovereignty, security	Requires encryption keys from service provider — useless if E2E encrypted
IT (Intermediary Guidelines) Rules, 2021	Mandates "traceability" — first originator of a message must be identifiable	WhatsApp challenged this in court; compliance undermines encryption
UAPA, 1967 (amended 2019)	Designate organisations and individuals as terrorists; investigate terror financing	Digital evidence admissibility rules still evolving
Telegraph Act, 1885 (Section 5)	Authorises interception of communications	Written for physical telegraphs; anachronistic for digital age

The Traceability Debate

The IT Rules 2021 require messaging platforms with **5 million+ users** to enable **traceability** — identifying the first originator of a message flagged as harmful. This creates a fundamental tension:

- **Government's argument:** Traceability is essential to identify terror recruiters, misinformation spreaders, and child abuse material circulators
- **Platform's argument (WhatsApp):** Traceability requires breaking E2E encryption for all users, which undermines privacy and security for everyone
- **Supreme Court:** The case is pending; no final ruling yet

CONSTITUTIONAL BALANCE

The editorial frames the issue as a conflict between:

- **Article 21 — Right to Privacy** (Puttaswamy judgment, 2017): Privacy is a fundamental right; any restriction must satisfy the proportionality test (legitimate aim, necessity, minimal intrusion)
- **Article 19(1)(a) — Freedom of Speech**: Includes the right to communicate privately
- **Article 19(2) — Reasonable Restrictions**: In the interests of sovereignty, integrity, security of the state, public order

The **Puttaswamy proportionality test** requires that any surveillance or interception measure must be:

- **Sanctioned by law**

Necessary (not merely convenient)

Proportionate to the legitimate aim

Subject to **procedural safeguards** against abuse

INTERNATIONAL APPROACHES

Country	Approach
Australia	Assistance and Access Act, 2018 — companies must help law enforcement access encrypted data; can be compelled to build backdoors
UK	Investigatory Powers Act, 2016 (Snoopers' Charter) — authorises bulk data collection; companies can be required to remove encryption
EU	CSAM Regulation (proposed) — "chat control" requiring platforms to scan encrypted messages for child abuse material; heavily debated
USA	No mandate to break encryption; FBI repeatedly calls for "responsible encryption" with law enforcement access
India	IT Rules 2021 traceability mandate; under legal challenge

UPSC RELEVANCE

IT Act Section 69, IT Intermediary Guidelines 2021 (traceability), UAPA 2019 amendments, Puttaswamy judgment (2017), Article 19(2) reasonable restrictions.

MAINS GS2:

Balancing privacy and security; role of judiciary in mediating fundamental rights conflicts; India's counter-terrorism legal architecture.

MAINS GS3:

Internal security challenges from encrypted platforms; cyber terrorism; role of technology in national security.

MAINS GS4:

Ethical dilemmas in mass surveillance vs individual privacy; whistleblower protection vs national security.

📌 FACTS CORNER — KNOWLEDGEPEDIA

LEGAL FRAMEWORK:

IT Act, 2000 (Section 69): government interception powers

IT Intermediary Guidelines, 2021: traceability mandate (5M+ user platforms)

UAPA, 1967 (amended 2019): individual designation as terrorist

Telegraph Act, 1885 (Section 5): communication interception

Puttaswamy v. Union of India (2017): privacy is fundamental right under Article 21

ENCRYPTED PLATFORMS:

WhatsApp: E2E encrypted; Signal protocol; metadata available

Signal: E2E; minimal metadata; open-source

Session: onion routing + E2E; no phone/email needed; decentralised

Telegram: optional E2E (Secret Chats only)

INTERNATIONAL:

Australia: Assistance and Access Act, 2018 (can compel backdoors)

UK: Investigatory Powers Act, 2016 (bulk data collection)

EU: CSAM Regulation proposed (chat control debate)

KEY CONSTITUTIONAL PROVISIONS:

Article 19(1)(a): freedom of speech (includes private communication)

Article 19(2): reasonable restrictions (sovereignty, security, public order)

Article 21: right to privacy (Puttaswamy, 2017)

Proportionality test: sanctioned by law, necessary, proportionate, safeguarded

Sources: The Hindu , InsightsOnIndia

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

in linkedin.com/in/epicbharat

📖 Read Full Article on Ujiyari →

https://ujiyari.com/editorials/2026/03/encrypted-platforms-digital-terrorism/

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