The Threat of Digital Tradecraft in Terrorism

Mains: *GS III – Challenges to Internal Security through Communication Networks*

Why in News?

Recently, a car explosion near Delhi's Red Fort on November 10, killing at least 15 people and injuring over 30, has revealed the use of advanced digital tradecraft in terrorist attacks.

What were the major findings of the investigation?

- **Encrypted communication –** The trio is alleged to have communicated via the *Swiss messaging app Threema*, a platform known for its high privacy design.
- Threema does not require a phone number or email to register, instead it assigns users a random user ID unlinked to any personal identifier.
- Investigators suspect that the three accused may have established their own private Threema server, creating a closed, isolated network through which they shared maps, layouts, documents, and instructions.
- The server may have been hosted either within India or abroad (investigations are ongoing as to its origin).

Threema's architecture *is particularly useful to evade detection because it offers end-to-end encryption, no storage of metadata, and allows message deletion from both ends.*

- These features make it extremely difficult for digital forensics teams to reconstruct full communication chains.
- **Sharing information using 'dead-drop emails' –** In what is being described as a classic "spy-style" technique, the suspects apparently used a shared email account (accessible to all module members) to communicate via unsent drafts.
- Instead of sending messages, they would save drafts; another member would log in, read or update them, and delete them — leaving no outgoing or incoming record on conventional mail logs.
- This method, sometimes referred to as a "dead drop," is particularly insidious because it generates almost no digital footprint.
- **Reconnaissance and ammunition stockpiling –** As per interrogations and forensic data, the accused conducted multiple recce missions in Delhi before the attack.
- Investigators allege that ammonium nitrate, a powerful industrial explosive, was stockpiled, possibly via a red EcoSport vehicle that has now been seized.
- The use of a familiar vehicle, rather than something more suspicious, may have helped the module remain under the radar during logistics buildup.
- **Operational discipline and external linkages –** Sources suggest that Dr. Umar,

who was reportedly the driver of the car that caused the blast, "switched off his phones" and cut digital ties after the arrest of his associates, a sophisticated tactic to limit exposure.
- Moreover, though investigations are ongoing, some sources suggest that the attack has links with the Jaish-e-Mohammed (JeM) or was following a JeM-inspired module.
- **The layered communication architecture** — Encrypted apps, dead-drop emails, coupled with infrequent but deliberate physical recces, suggests a cell that counts operational security among its highest priorities.

What are the implications?

- **Surveillance ineffectiveness** – As more terror modules adopt privacy-preserving technologies, traditional surveillance such as phone tapping, metadata collection, and email intercepts have become less effective.
- This should force law enforcement agencies to rethink investigative architectures.
- **Use of banned apps and proxies** – Threema is reportedly banned in India *(under Section 69A of the Information Technology Act, 2000),* yet the suspects seem to have continued using it via VPNs and foreign proxies.
- This suggests that bans alone may not stem the misuse of such apps, especially by sophisticated operators.
- Investigators need advanced capabilities such as being able to track private servers, reverse engineer encrypted networks, and apply memory forensics to trace such modules.
- Standard device seizures may not be sufficient without specialised technical expertise.
- **Potential of big network** – Moreover, if a link to external handlers (such as the JeM) is proved to be true, this attack may be part of a wider network.
- The level of planning and security discipline shown suggests not a lone cell, but a well-trained, possibly transnational, group.

What are some policy solutions?

- **Build a dedicated digital forensics teams** – There is a necessity to establish and expand teams skilled in encrypted-platform analysis, server forensics, and memory dumping to recover ephemeral data.
- The government should invest in units that specifically monitor misuse of E2EE platforms, anonymising services, and VPN exit nodes for potential terror tradecraft.
- **Regulation of self-hosted communication infrastructure** – The state needs to craft regulatory frameworks mandating private servers hosting communication platforms to comply with lawful access obligations, while balancing privacy rights.
- Cooperation with technology providers needs to be encouraged in order to enable lawful interception under strictly controlled, judicially-supervised processes.
- **Legal frameworks need to be enhanced** – Counter-terrorism laws need to be updated so that it explicitly addresses threats posed by encrypted, decentralised communication.
- Introduce or refine digital dead-drop detection mechanisms in investigations.
- Law enforcement should be trained to look for shared accounts, draft-only mailboxes, and similar tradecraft.

- **Prioritising community and institutional engagement** – The fact that the suspects were reportedly doctors from a university is deeply concerning; such institutions need support to detect radicalisation early.
- Counter-radicalisation programs tailored to highly educated recruits may be deployed.
- Modules operating in professional spaces (doctors, academics) are often less visible, but may wield more technical or ideological sophistication.
- **Strengthening International collaboration** – Given the possible transnational nature (encrypted apps, private servers, cross-border funding) of the attack, the state should deepen cooperation with foreign intelligence and law enforcement agencies.
- It should also encourage tech diplomacy, and engage with countries where encrypted-messaging apps like Threema are based to explore lawful but privacy-respecting access to self-hosted infrastructure linked to terror cases.
- There should also be public awareness about how modern terror cells operate.

What lies ahead?

- The Red Fort blast investigation illustrates how modern terrorist modules are evolving rapidly.
- They no longer rely solely on brute force or mass propaganda they are integrating advanced digital tradecraft with traditional radicalisation and operational planning.
- These developments resonate strongly with academic insights into extremist behaviour in the digital age.
- As violent actors become more technically adept, states too must adapt , not just by strengthening brute-force capacity, but by cultivating sophisticated, multidisciplinary intelligence, cyber-forensics, and legal tools.
- For India and democracies globally, this case is a sobering reminder that the next frontier in counter-terrorism is not just on the physical terrain, but also in encrypted, decentralised, and deeply private digital spaces.
- If we are to safeguard our cities and societies, we must meet this threat not only on the streets and borders, but also on servers and in code.

Reference

[The Hindu| Digital Tradecraft in Terrorism]