

# Cross-Border Cybercrime

Posted at: 15/07/2025

## Cross-Border Cybercrime: India's Emerging National Security Challenge

---

### Context:

India is facing an alarming surge in **cyber frauds** originating from **Southeast Asia**. Between **January and May 2025**, the **Ministry of Home Affairs (MHA)** reported that **over ₹7,000 crore** was lost to such scams. The Indian Cyber Crime Coordination Centre (**I4C**) has traced a majority of these scams to **organized networks based in Myanmar, Cambodia, Vietnam, Laos, and Thailand**.

---

### Southeast Asia-Based Cyber Scams: Scope and Scale

- **Over 50%** of the ₹7,000 crore cyber scam losses in early 2025 were traced to **Southeast Asian countries**.
  - India is reportedly losing around **₹1,000 crore every month** to these scams.
  - Scam centres are allegedly **operated by Chinese-controlled syndicates**.
  - These syndicates use **high-security compounds** to carry out operations.
- 

### Forced Labour and Human Trafficking

- Over **5,000 Indians** have reportedly been **trafficked** and **forced to work** in scam centres.
- Victims from **Africa, Asia, Europe, and the Americas** have also been identified in these operations.

- Testimonies from rescued individuals revealed several **trafficking routes** involving:

- **Dubai → China → Cambodia**
  - **Tamil Nadu → Cambodia**
  - **Maharashtra → Thailand → Cambodia**
  - **Delhi → Bangkok → Cambodia**
  - **Kerala → Singapore/Vietnam → Cambodia**
  - **Kolkata → Vietnam → Cambodia (via road)**
- 

### Identified Scam Hotspots

- Intelligence and survivor reports have identified:

- **45 scam centres in Cambodia**
  - **5 centres in Laos**
  - **1 centre in Myanmar**
- 

### Types of Cyber Frauds Identified

#### 1. Stock Trading and Investment Scams

- Promise of **high returns** in stock markets, cryptocurrency, or mutual funds.
- Victims contacted via **social media, WhatsApp, or fake apps**.
- Scammers **pose as financial advisors** and show **fake profits** to attract larger investments.
- Once substantial money is deposited, **scammers disappear**.

## 2. Digital Arrest Scams

- Victims receive **fake calls or video calls** from impersonators of **CBI, IT Department, or Police**.
- They are falsely informed that their **identity or bank account** is linked to crimes like **money laundering or drug smuggling**.
- **Threats of arrest** are used to extort money in the form of "**security deposits**" or **fin**es.

## 3. Task-Based and Investment Scams

- Victims are offered **online jobs or freelance tasks** (e.g., liking videos, app ratings).
- **Small payments** are made initially to build trust.
- Later, victims are asked to **invest money** with promises of higher returns. Once they do, the scammers **vanish**.

---

## Recruitment of Indians for Scam Operations

- Agents recruiting Indians have been traced to:
  - **Maharashtra**
  - **Tamil Nadu**
  - **Uttar Pradesh**
  - **Delhi**
  - **Jammu & Kashmir**

---

## Government Response and Action Taken

- An **inter-ministerial panel** has been formed to address vulnerabilities in:
    - **Banking systems**
    - **Telecom infrastructure**
    - **Immigration processes**
  - The **CBI** has registered **FIRs** against **Point of Sale (PoS) agents** issuing **ghost SIM cards** used in these scams.
- 

## Conclusion

This cybercrime surge reflects the growing **transnational nature of digital fraud**, requiring enhanced **international cooperation**, **border control**, and **cybercrime tracking** mechanisms. India's response will need a **multi-pronged approach**, including **legal reform**, **public awareness**, and **global coordination**, to curb the rising menace.

