

Hoax Bomb Threats

Posted at: 28/10/2024

India's Fight Against Hoax Bomb Threats on Social Media

Context :

- The Ministry of Electronics and Information Technology (MeitY) issued an **advisory to social media platforms**, urging them to take accountability in curbing threats against flights operating from India.
 - The advisory stressed the **uncontrolled spread of hoax bomb threats** via forwarding, resharing, and reposting features on social media platforms.
-

Advisory to Address Hoax Bomb Threats on Social Media

Recent Hoax Bomb Threats Impacting Airlines:

- **Disruptions to Indian Airlines:** In the last two weeks, Indian carriers, including Air India, Vistara, Air India Express, Indigo, Alliance Air, and Star Air, faced a series of hoax threats.
- These incidents led to **emergency responses**, rerouting of flights, and even military fighter jet intercepts, especially when emergency transponder codes were triggered in international airspace.
- Despite being hoaxes, the threats caused **delays and financial losses** estimated at ₹13-₹17 lakh per hour for the airlines.

Origin and Nature of Threats:

- Most threats originated on **social media**, according to the government. Intelligence agencies are investigating these threats, focusing on tracking **IP addresses** and **VPN usage**.
 - While **initial** threats appeared to be hoaxes, authorities are cautious, given the scale of India's **4,000 daily flight operations**.
 - Since the start of these incidents, approximately **275 threats have affected around 48,000 flights**.
-

Aviation Security Framework

1. ICAO's Aviation Security Directives:

- India's aviation security guidelines align with the **International Civil Aviation Organization's (ICAO) Annex 17 on Aviation Security**, which mandates global

measures against interference in civil aviation.

- The ICAO **Aviation Security Manual (Doc 8973)** provides member states with detailed security procedures and is regularly updated to counter evolving threats.

2. Security Agencies and Measures in India:

- In India, the **Bureau of Civil Aviation Security** sets security standards for civilian flights, while the **Directorate General of Civil Aviation (DGCA)** oversees flight safety.
- Additional agencies involved include the **Airports Authority of India, CISF, NSG, IB, RAW**, and the **Ministry of Home Affairs**.

3. Proposed Legal Amendments to Strengthen Aviation Security:

- In response to recent security threats, amendments are being considered for the **Aircraft Act 1934, Aircraft Rules 1937**, and related laws.
- Planned updates include **stricter penalties, no-fly list provisions**, and **expanded legal recourse** for security breaches.
- Proposed updates to the **Suppression of Unlawful Acts against Safety of Civil Aviation Act, 1982** would further strengthen responses to in-flight and on-ground threats.

Challenges in Handling Security Threats

1. Systemic Issues:

- While details remain undisclosed, the recent incidents reveal **systemic gaps in procedures, training, technology, communication**, and regulatory enforcement within aviation security.

2. Recommended Technological Investments:

- Experts recommend **advanced call tracking, AI-powered call analysis, voice stress analysis**, and threat assessment systems to address hoax threats.
- Emerging technologies, such as **quantum computing** and **aviation cybersecurity frameworks**, could bolster security.
- **AI-powered chatbots** for preliminary threat assessments and profiling could help understand motivations and threat levels.

3. Deterrence and Awareness Strategies:

- Experts suggest publicly displaying **photos of offenders** on social media and at airports as a deterrent.
- They also recommend creating a **global hoax call database** and offering **rewards for informers** to encourage reporting of hoax threats.

About the Advisory

MeitY's Advisory on Social Media Compliance:

- MeitY has advised all social media platforms to comply with the **Information Technology (IT) Rules** and **Bharatiya Nyaya Sanhita (BNS)** by making significant efforts to **promptly remove bomb threat posts**. Non-compliance could lead to legal accountability.

Legal Framework:

- The advisory relies on provisions of the **IT Act, 2000** and **IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**, mandating intermediaries to remove harmful misinformation.
- Previously, these provisions were invoked to tackle deepfake content under **Rule 3(1)(b) of the IT Rules**, which prohibits **false and misleading information**.

Potential Consequences for Non-Compliance:

- Non-compliant platforms risk losing **intermediary liability protections**, subjecting them to legal action as publishers of harmful content.
- The Ministry emphasized that legal actions could be pursued under both the **IT Act** and the **Bharatiya Nyaya Sanhita, 2023** if due diligence is not maintained.

