Cybercrime and the Crisis of Global Governance

Published On: 27-01-2026

In News: India has **not signed the UN Convention against Cybercrime (2024)**, highlighting **deep fractures in global cyber governance**. The episode reflects tensions between **global cyber norms** and **national sovereignty**, especially in a **polycentric digital order**.

What is the Crisis of Global Cyber Governance?

Refers to the **growing gap between universal international principles** and **fragmented national implementation**.

While countries agree on broad goals (e.g., tackling cybercrime, safe AI, child protection), they **diverge on rules, enforcement, and data access**.

Leads to **polycentricism**:

oMultiple overlapping, sometimes conflicting regional, bilateral, and national cyber regimes.

oWeakens uniform global enforcement against transnational cybercrime.

Key Trends in Cybercrime (India-Focused)

1. Surge in Cyber Incidents

- Cybercrime cases rose from **10.29 lakh (2022)** to **22.68 lakh (2024)**.
- Reflects growing digital penetration and weak cross-border enforcement.

2. AI-Powered Cyber Attacks

- AI acts as a **force multiplier**:
- Sophisticated phishing
- Deepfake-enabled financial fraud
- Automated malware deployment

3. Evolution of Ransomware

- New-age ransomware involves:
- Data theft + encryption
- Multi-stage extortion
- Psychological pressure
- Increasingly targets **small and medium organisations** with limited cyber capacity.

4. Financial Impact

- India lost **~?1,000 crore per month** to cyber frauds in H1 2025.
- Annual losses could reach **0.7% of GDP**, posing macroeconomic risks.

5. Identity-Centric Threats

- Identity security is now the **primary attack surface**.
- Deepfakes and credential abuse bypass:
- Biometrics
- Traditional perimeter-based cyber defences

UN Convention against Cybercrime (Hanoi Convention)

Key Features

- **First universal treaty** on cybercrime.
- Criminalises:
- Ransomware
- Financial cyber fraud
- Non-consensual sharing of intimate images
- Enables **cross-border electronic evidence sharing**.
- Creates a **24/7 global cooperation network** for investigations.
- Includes **human rights safeguards**, though critics question their robustness.
- **First global treaty** to specifically address **online sexual violence against children**.

India’s Concerns

- Potential dilution of **institutional autonomy**.
- Data access and sovereignty issues.
- Human rights safeguards tied to **domestic legal frameworks**, raising misuse concerns.

Other Global Cyber Governance Initiatives

1**Budapest Convention (2001)**

- European-led cybercrime treaty.
- **76 parties**, widely operational.
- Criticised as **non-inclusive**; India, Russia, China are not signatories.

2**Hiroshima Process (G7)**

- Focuses on **safe and responsible generative AI**.
- Emphasises global standards and risk mitigation.

3**UN Global Digital Compact**

- Seeks a **safe, inclusive, and human-centric digital future**.
- Addresses digital trust, governance, and access.

4**Cyber Initiative Tokyo 2025**

- Explores **data security**, **critical infrastructure protection**, and **AI-era deterrence**.