ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

Cyber Warfare is Outpacing Global Legal Accountability

THE HINDU

23 May 2026 · SECURITY & DEFENCE · IR · SCIENCE & TECH · GS3 · GS2

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Cyber Warfare is Outpacing Global Legal Accountability

The Hindu 23 May 2026 GS3 GS2

TH The Hindu | 5 tags

INTERVIEW ANGLE

"If you were heading India's delegation at the UN Open-Ended Working Group on cybersecurity, what three norms would you push for, and why is binding attribution so difficult?"

The Tallinn Manual is non-binding, the UN GGE-OEWG twin track has produced norms without enforcement, and the Budapest Convention remains unsigned by India and most other large non-European powers. Meanwhile cyber operations against critical infrastructure — from SolarWinds and Volt Typhoon abroad to Kudankulam and AIIMS Delhi at home — continue at industrial pace. The next OEWG cycle, the pending Indian National Cyber Security Strategy and India's 2026-28 chairing of the Common Criteria Development Board are the moment to push for a binding framework.

THE ACCOUNTABILITY GAP

Between 2019 and 2025, the public catalogue of cyber operations against critical infrastructure expanded sharply. The **SolarWinds** supply-chain compromise disclosed in December 2020 affected US federal agencies and major private firms. The **Colonial Pipeline** ransomware incident of May 2021 halted fuel supply on the US east coast for days. The Microsoft Threat Intelligence Centre disclosed **Volt Typhoon** in May 2023 — a China-state-linked campaign targeting US critical infrastructure, further detailed in CISA-Five Eyes advisories in 2024.

India's catalogue is no shorter. In September 2019 the **Kudankulam Nuclear Power Plant** suffered a malware intrusion (the DTrack family) attributed to a North Korea-linked group; in November 2022, **AIIMS Delhi** was hit by a ransomware attack that crippled patient services for days. Indian Railways, pharmaceutical majors and State data centres have all reported intrusions in the same window. The operations are not academic. The accountability is.

A PATCHWORK OF NORMS

The international architecture today rests on three uneven pillars.

1. The Tallinn Manuals

The **Tallinn Manual on the International Law Applicable to Cyber Warfare** (1.0, 2013) and the **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations** (2017) were prepared by international groups of experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Tallinn, Estonia. **Tallinn Manual 3.0** is currently under preparation.

The Manuals are restatements — they describe how existing international law (UN Charter, jus ad bellum, international humanitarian law, human rights law) *applies to* cyber operations. They are not treaties. They have no signatories. They reflect, broadly, the perspective of NATO and like-minded States, which limits their political authority outside that bloc.

2. The UN Twin Track: GGE and OEWG

BODY	ESTABLISHED	MEMBERSHIP	OUTPUT
Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security	2004 (first GGE)	Limited (25 States in the latest cycle)	Six reports (2010, 2013, 2015, 2017 — no consensus — 2021); 2013 consensus that international law applies in cyberspace; 2015 list of eleven voluntary norms
Open-Ended Working Group (OEWG) on developments in ICTs	Established 2019 (proposed by Russia)	All UN member States	First cycle 2020-21 final report; second cycle 2021-25; next cycle 2026-30 expected

The GGE-OEWG twin track represents a hard-fought compromise between the US-EU preference for a limited expert process and the Russia-China preference for a universal process. It has produced influential norms — including the protection of critical infrastructure, due diligence, and non-interference — but no binding instrument and no enforcement mechanism.

3. The Budapest Convention

The **Council of Europe's Convention on Cybercrime** (Budapest, 2001) entered into force in 2004 and has been ratified by over 70 States. It harmonises substantive cybercrime offences (illegal access, data interference, computer-related fraud), procedural powers (preservation, search, seizure) and international cooperation (mutual legal assistance, 24/7 contact points).

India has not signed the Convention. The principal concern is **Article 32(b)**, which permits a State party to access stored computer data in another State's territory "with the lawful and voluntary consent" of the person legally authorised to disclose it — without prior recourse to mutual legal assistance. Indian negotiators have read this as a derogation from territorial sovereignty over data. Russia and China hold similar concerns; both have pushed for a separate UN cybercrime convention process.

WHY BINDING RULES HAVE PROVED ELUSIVE

Three structural disagreements stall any binding instrument:

Bloc politics. A Russia-China grouping favours an approach grounded in State sovereignty over information content and a UN-anchored treaty. A US-EU grouping prefers the GGE process and the Tallinn approach, anchored in existing international law.

Definitional gaps. What is a "cyber-attack"? What is a "cyber-weapon"? When does a cyber operation cross the threshold of a "use of force" under Article 2(4) of the UN Charter, or an "armed attack" triggering self-defence under Article 51? Different States draw the lines differently.

Attribution. Technical attribution is now reasonably mature for sophisticated incidents — but legal-political attribution requires a State willing to publicly accuse another State, with evidence that can survive denial. The use of proxies, false flags and third-country infrastructure makes attribution by State A almost always contestable by State B.

INDIA'S DOMESTIC ARCHITECTURE

India's legal and institutional framework for cybersecurity rests on several overlapping pillars:

PILLAR	AUTHORITY	ROLE
Information Technology Act, 2000 (and amendments)	MeitY	Core statute for cybercrime and electronic governance
Digital Personal Data Protection Act, 2023	MeitY	Personal data protection
CERT-In	Section 70B, IT Act; MeitY (est. 2004)	National incident response, advisories
NCIIPC (National Critical Information Infrastructure Protection Centre)	Section 70A, IT Act; NTRO	Protection of notified Critical Information Infrastructure (CII)
I4C (Indian Cybercrime Coordination Centre)	MHA (est. 2018)	Coordination of cybercrime response across States
National Cyber Security Coordinator	PMO	Strategic coordination
National Cyber Security Policy 2013	MeitY	Policy framework (revision pending)
National Cyber Security Strategy	Draft, pending finalisation	Successor strategy

The **Critical Information Infrastructure** notified under Section 70 covers power, banking, telecom, transport, government, and strategic & public enterprises. Operationally, NCIIPC issues guidance, audits and threat intelligence to these sectors.

INDIA IN THE WORLD: A BRIDGING POSITION

India sits — usefully — between the two blocs. It is a constructive participant in both the GGE and the OEWG. It has not signed the Budapest Convention but engages with it. It has signed onto the **Common Criteria Recognition Arrangement (CCRA)** for cybersecurity product certification since 2013, and is scheduled to **chair the Common Criteria Development Board (CCDB) for 2026-28**. It participates in BRICS and SCO cyber dialogues. It runs bilateral cyber dialogues with the US, Russia, Japan, France, the UK, the EU and others.

This bridging position — distinct from both the NATO axis and the SCO axis — is a real asset. It allows India to argue for binding norms that protect civilian critical infrastructure (a near-universal concern), capacity-building for developing countries (a Global South concern), and clearer attribution standards (a procedural concern shared across blocs).

WHAT AN INDIAN AGENDA SHOULD PUSH

1. **Binding protection of civilian critical infrastructure.** Convert the GGE 2015 voluntary norm on critical infrastructure into a binding rule, with a clear list of protected sectors (power, water, health, financial, electoral).
2. **Attribution standards.** Push for an international code on attribution — what evidence threshold, what publication procedure, what consequences flow from a finding.
3. **Budapest Convention with reservations.** Reopen the question of acceding to the Budapest Convention with a declaration limiting Article 32(b)'s cross-border data access, in exchange for full access to its mutual legal assistance infrastructure.
4. **Global South capacity-building.** Use the 2026-28 CCDB chair to anchor a developing-country capacity-building track — product certification, CERT-to-CERT cooperation, training pipelines.
5. **Finalise the National Cyber Security Strategy.** A binding international agenda is hollow without domestic readiness; the long-pending Strategy must be finalised and resourced.

UPSC MAINS ANALYSIS

GS Paper 3 — Internal Security. This is core syllabus territory: cyber security, basics of cyber-attacks, role of CERT-In and NCIIPC, protection of critical infrastructure under Section 70, IT Act 2000.

GS Paper 2 — International Relations. The editorial maps the international regime — Tallinn Manual, UN GGE, OEWG, Budapest Convention — and India's bridging role between NATO and SCO groupings, illustrating institution-building in a contested domain.

Conceptual bridge. The cyber-norms gap is a textbook case of how technology outpaces law. The institutional response — binding rules, attribution standards, capacity-building — is the same template India will need for AI, autonomous weapons, and space.

Prelims Facts Corner

ITEM	FACT
Tallinn Manual 1.0	2013, by NATO CCDCOE
Tallinn Manual 2.0	2017
Tallinn Manual 3.0	Under preparation
UN GGE established	2004; six reports between 2010 and 2021
GGE consensus on applicability of international law	2013
GGE voluntary norms	Eleven, in 2015
OEWG established	2019, by UN General Assembly resolution
Budapest Convention	Council of Europe, opened 2001, in force 2004
India signatory to Budapest Convention	No
CERT-In	Section 70B, IT Act; under MeitY
NCIIPC	Section 70A, IT Act; under NTRO
I4C	Under MHA, 2018
DPDP Act	2023
Common Criteria Development Board	India to chair 2026-28

> *Cyber operations are at industrial pace; cyber law is at glacial pace. The next OEWG cycle, India's CCDB chair and the long-pending National Cyber Security Strategy together offer a rare alignment of moments. If India does not use them to push for binding protection of civilian critical infrastructure and clearer attribution standards, the next Kudankulam, the next AIIMS, will be answered — once again — by silence.*

Sources: The Hindu , PRS , PIB

KEY ARGUMENTS AT A GLANCE

The pace of state-backed cyber operations now far exceeds the pace at which international law for cyberspace is being settled; the Tallinn Manual is non-binding, the UN GGE-OEWG twin track has produced norms without enforcement, and the Budapest Convention remains unsigned by most large powers including

India — leaving attribution, response and redress to ad hoc state practice.

✓ SUPPORTING

- The Tallinn Manual 1.0 (2013) and 2.0 (2017), produced by the NATO Cooperative Cyber Defence Centre of Excellence, are scholarly restatements of how existing international law applies to cyber operations; they have no treaty force, and Manual 3.0 is still under preparation.
- The UN Group of Governmental Experts produced six reports between 2004 and 2021, including the consensus that international law applies in cyberspace (2013) and the eleven voluntary norms of responsible state behaviour (2015); the parallel Open-Ended Working Group, established in 2019, broadens participation but has likewise produced no binding instrument.
- The Council of Europe's Budapest Convention on Cybercrime (2001) — the principal multilateral instrument — has been ratified by over 70 States but not by India, Russia or China, partly because Article 32(b) permits cross-border access to stored data with consent, raising sovereignty concerns.
- Major cyber incidents — SolarWinds (2020), Colonial Pipeline (2021), Volt Typhoon (disclosed by Microsoft May 2023, further detailed in 2024 Five Eyes advisories) — and India-specific incidents at the Kudankulam Nuclear Power Plant (2019) and AIIMS Delhi (November 2022) show that the operational pace of state and state-linked cyber activity has outrun the normative framework.

⚠ COUNTER

Some States and scholars argue that a binding treaty is premature, that customary international law combined with voluntary norms allows flexibility, and that a hard treaty risks freezing immature definitions of "cyber weapon", "cyber-attack" and "critical infrastructure" into law that may not survive the next decade of technology.

→ WAY FORWARD

India should remain active in both the GGE and the OEWG, push for a binding instrument that clarifies attribution standards and protects civilian critical infrastructure, reconsider accession to the Budapest Convention with declarations on Article 32(b), and use its 2026-

28 chairing of the Common Criteria Development Board to anchor a Global South capacity-building agenda.

🧠 **PRACTICE TODAY'S QUIZ**

Take the 23 May 2026 Quiz →

✍️ MAINS ANSWER FRAMEWORK

QUESTION

Cyber operations between states are routine; binding international law to govern them is not. Examine the gaps in the present cyber-norms architecture — Tallinn Manual, UN GGE and OEWG, Budapest Convention — and outline a realistic Indian agenda for the next cycle of negotiations. (250 words)

INTRODUCTION

A series of disclosed cyber operations against critical infrastructure — from SolarWinds and Colonial Pipeline to Volt Typhoon and India's own Kudankulam and AIIMS Delhi incidents — has made one fact clear: state-linked cyber activity now operates at a tempo that international law has not caught up with. The gap between operation and accountability is the central foreign-policy and security-policy challenge of the decade.

BODY

The architecture of cyber norms today rests on three uneven pillars. First, the Tallinn Manuals (1.0 in 2013, 2.0 in 2017, 3.0 under preparation), produced by NATO's Cooperative Cyber Defence Centre of Excellence, are scholarly restatements of how existing international law — jus ad bellum, jus in bello, human rights law — applies to cyber operations; they are non-binding and reflect a primarily Western consensus.

Second, at the United Nations, the Group of Governmental Experts (GGE) produced six reports between 2004 and 2021, including the landmark 2013 consensus that international law applies in cyberspace and the 2015 set of eleven voluntary norms of responsible state behaviour; the parallel Open-Ended Working Group (OEWG), launched in 2019 and continuing through the next 2026-30 cycle, broadens participation but has so far been unable to convert norms into a binding instrument. Third, the Council of Europe's Budapest Convention on Cybercrime (2001), the only multilateral treaty in force, has not been signed by India, Russia or China.

Attribution remains the deepest technical and legal problem — proxies, false flags, third-country infrastructure and differential evidentiary standards all combine to let states deny operations even after

technical attribution is relatively settled. India's own framework — the IT Act 2000, CERT-In (Section 70B), NCIIPC (Section 70A), the I4C under the MHA, the DPDP Act 2023 and the still-pending National Cyber Security Strategy — needs an external anchor in binding international law; without it, domestic safeguards are perpetually on the defensive.

CONCLUSION

India's emerging position — active in both the GGE and OEWG, chair of the Common Criteria Development Board for 2026-28, a credible voice for the Global South — should be deployed to push for a binding cybersecurity instrument that protects civilian critical infrastructure, clarifies attribution standards, and provides capacity-building for developing economies. Cyber accountability cannot remain a matter of voluntary norms when the operations are plainly compulsory in their effects.

RELATED DAILY ARTICLES

23 May Current Affairs Today — May 23, 2026

23 May India Test-Fires Agni-1 Ballistic Missile from...

23 May Saudi Arabia Joins International Big Cat Alliance as...

23 May India Blocks China's WTO Dispute Panel Request on Solar...

← NEWER EDITORIAL
For India, Weakening Monsoon and Fertiliser Crisis: A Double...

OLDER EDITORIAL →
In Xi and Putin's 'No Limits' Partnership, a Growing...

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Read Full Article on Ujiyari →

https://ujiyari.com/editorials/2026/05/hindu-cyber-warfare-international-law-tallinn-2026/