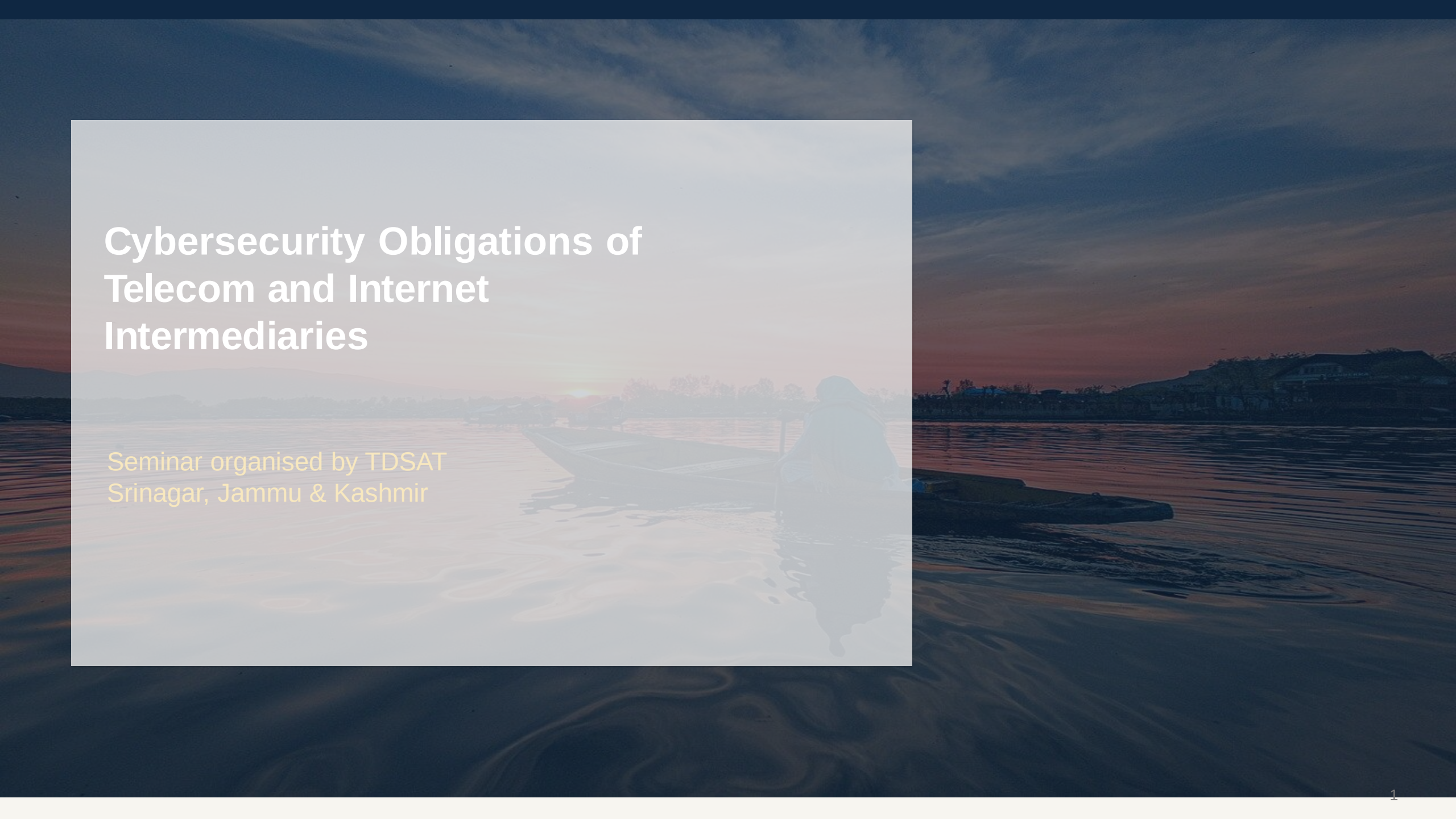


A person in a boat on a lake at sunset. The person is wearing a dark shawl and is seen from behind, rowing the boat. The water is calm, reflecting the sunset sky. In the background, there are some buildings and trees on the shore.

Cybersecurity Obligations of Telecom and Internet Intermediaries

Seminar organised by TDSAT
Srinagar, Jammu & Kashmir

Why this topic matters now

Connectivity has become critical infrastructure

I. Context

The digital layer now carries:

- banking and payments
- governance and public services
- health and education
- emergency communications
- identity and trust

Three reasons cybersecurity is now a legal issue

Scale

A telecom or platform failure can affect entire populations, not just individual users.

Speed

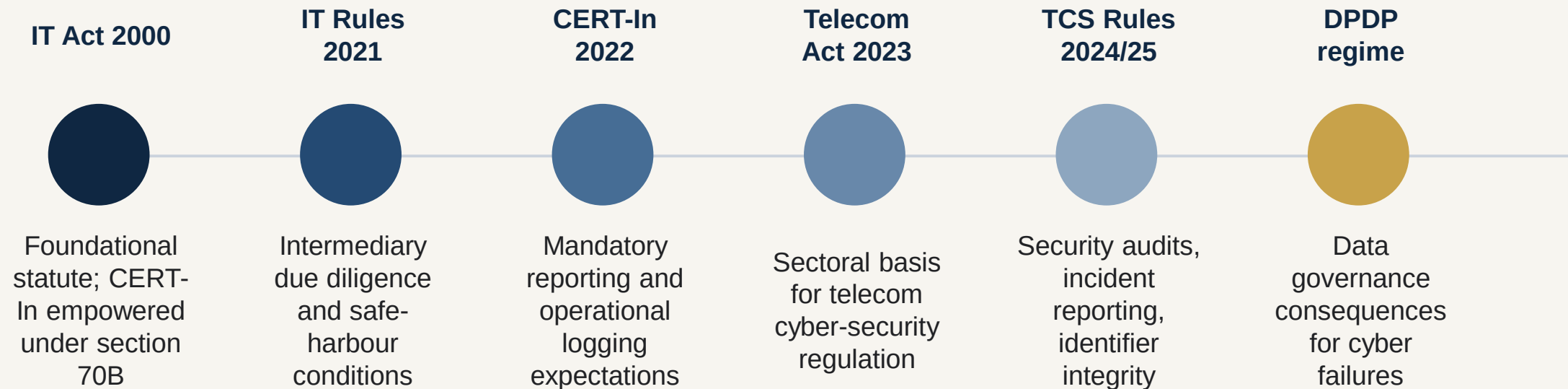
Cyber incidents escalate quickly; delayed response may itself amount to non-compliance.

Trust

Users, regulators and courts increasingly expect provable security governance.

The current legal architecture

Different layers of regulation now converge on cyber resilience



The obligations differ by role, but the burden of responsibility is shared.

Telecom entities: the core security burden

Carriage-layer integrity affects networks, consumers and the State

III. Telecom

Telecom-facing obligations now centre on:

- regular security audits and cross-checks
- network hardening and vulnerability management
- supply-chain and access-control safeguards
- incident reporting and operational response
- protection of telecom identifiers and device integrity

Why the threshold is higher

A telecom compromise can produce service outages, interception risks, identity abuse, and cascading disruption across critical systems.

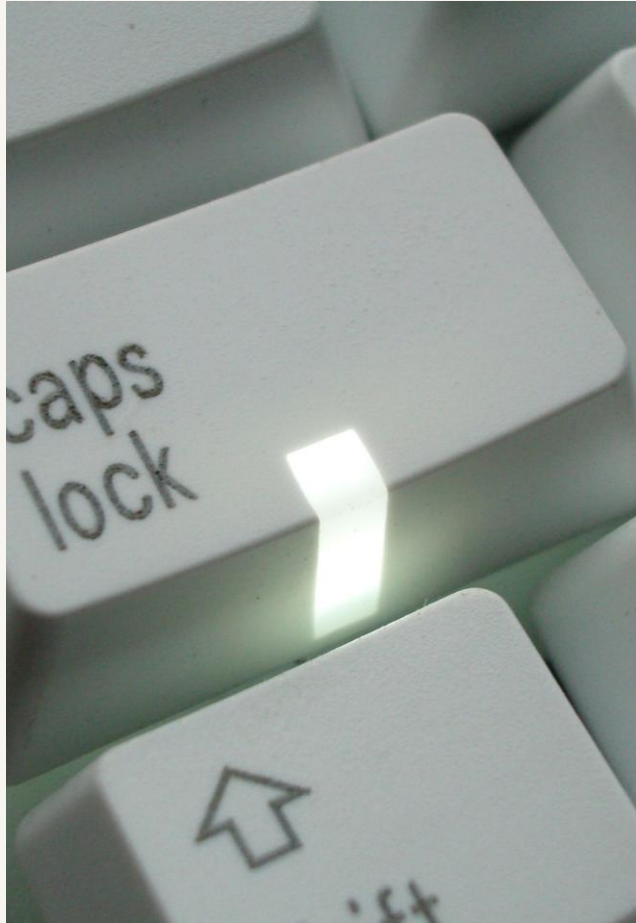
Key regulatory signal

The 2025 amendment press release expressly refers to regular security audits, incident reporting, and prohibition on IMEI tampering.

Incident reporting changed the compliance culture

V. Response

Preparedness now matters as much as prevention



1. Notice

Detect or be informed of a covered cyber incident.

2. Report

Share available information with CERT-In within 6 hours.

3. Supplement

Do not wait for perfect facts; add details later.

4. Record

Maintain logs, escalation trails and forensic readiness.

The six-hour rule signals that cyber incidents are no longer internal embarrassments to be quietly managed.

Cybersecurity is now inseparable from data governance

VI. Overlap

A single incident can trigger multiple legal consequences

The age of siloed compliance is over.

A single cyber incident may trigger telecom, intermediary, data-protection, consumer and dispute-resolution consequences at once.

Contracts & consumers

Service commitments, user trust, and downstream liability

DPDP regime

Personal data consequences and regulatory oversight

CERT-In

National reporting, logging and response expectations

Sectoral rules

Telecom and intermediary-specific obligations

Emerging pressure points

The threat model is wider than classic hacking

Synthetic media

Deepfakes, misleading SGI, and automated deception now directly engage intermediary due diligence.

Telecom identifiers

DoT has used the TCS framework to address misuse of identifiers in app-based communications.

Supply chain

Equipment integrity, trusted sources, and vendor controls matter to network security.

Operational readiness

The decisive question is often not whether a breach occurred, but how quickly it was escalated and contained.

Evidence for adjudication

Logs, audit trails and internal escalation records increasingly shape disputes and regulatory scrutiny.

What a balanced legal approach should look like

VIII. Balance

Firm, proportionate, rights-conscious and innovation-aware



Five institutional shifts

- Move cybersecurity from the IT department to the boardroom
- Judge compliance by records: logs, audits, response times, and escalation trails
- Coordinate sector regulators, CERT-In, law enforcement and adjudicatory bodies
- Support capacity-building for smaller providers and regional actors
- Ensure adjudication remains technologically literate and sector-sensitive

Closing thought

Cybersecurity obligations are ultimately obligations of public trust

In the digital era:

- sovereignty is defended not only at borders, but also in servers, switches, identifiers and platforms;
- consumer rights are imperilled not only by unfair contracts, but also by insecure design, breaches and impersonation;
- and justice is tested not only in courtrooms, but also in how law responds to fast-moving technological risk.

The real task is to build a compliance culture that is timely, credible, technologically informed and anchored in public trust.

Thank you.