



# The UN Cybercrime Convention: Its Impact on the “Liberal Cyber Order”

Event Summary

6 March, 2025

- CSEP hosted its 31<sup>st</sup> Foreign Policy and Security Studies Tiffin Talk on **The UN Cybercrime Convention: Its Impact on the “Liberal Cyber Order”** with **Arun Sukumar** and **Arindrajit Basu**. **Dr Sukumar** is an Assistant Professor of International Relations at Ashoka University and **Mr Basu** is a PhD candidate in the Faculty of Governance and Global Affairs at Leiden University, The Netherlands.
- The discussion focused on how Chinese and Russian proposals for the landmark United Nations (UN) Convention on Cybercrime attempt to challenge the liberal cyber order, how countries like India navigate competing ideas of sovereignty in foreign policy, and what big questions need to be asked as the world order changes rapidly.
- The discussant was **Gunjan Chawla**, Cyber Policy Expert. The talk was moderated by **Shruti Jargad**, Research Analyst, CSEP.
- The discussion included participants from Indian government institutions, various foreign diplomatic missions and embassies, media, academic institutions and think tanks from India and abroad.
- This series of closed-door research seminars is curated by **Constantino Xavier**, Senior Fellow, CSEP and **Shivshankar Menon**, Distinguished Fellow, CSEP. It focuses on contemporary, evidence-based research with policy relevance to bridge Delhi’s scholar-practitioner divide.

## Centring the Territorial State: The Challenge to the Liberal Cyber Order

The United Nations (UN) Convention on Cybercrime, adopted in December 2024, represents the first legally binding UN instrument on cybercrime and is therefore an arena for competing ideas about the basic DNA of cyberspace. As the convention opens for signatures, the speakers analysed how proposals from China and Russia to the convention’s Ad Hoc Committee (AHC) have tried to systematically reconfigure cybersecurity governance.

After empirical analysis of the proposals, the speakers argued that China and Russia wish to constrain their strategic adversaries who are advantaged by the liberal cyber order and empower the territorial state as the sole determinant of cybersecurity governance. Under the guise of cybercrime, both countries wish to shape policies and standards about data usage and storage. They also seek to exert more control over digital activities abroad that

bear on territorial concerns, and frame cross-border data flows as the exclusive domain of governments. A greater role for the territorial state compels private companies to give up data when asked, subordinating their autonomy to the state’s wishes. This state-centric view of ‘cyber sovereignty’ is not new but is spreading more widely especially as China wields extensive market power in the cybersphere. This debate centres India, whose neutrality on the UN Convention may reflect both an expansive view of state sovereignty and a desire to avoid distance with Western partners.

The speakers emphasised that proposals by China and Russia represent a transformation in how cyberspace is conceptualised. While they have not yet received significant support, the proposals are a serious challenge to the existing order. Other countries which would be needed to execute order-level change, including India, have acknowledged this challenge. Chinese and Russian rhetoric which focuses on development and stability, while reject-

ing explicit mentions of human rights, has appeal among many countries in the developing world. The proposals attempt to take advantage of the Global South's discontent with the current liberal international order. However, many countries—including India—have been neither ardently for nor against the proposals in favour of maintaining multi-alignment.

## Sovereignty and the Memory of Colonisation

The discussion then broadened to consider lawfare—the use of law for military objectives—and the memory of colonisation. Many former colonies still remember that colonisation itself had legal support and justification. One participant argued that the experience of lawfare may lead postcolonial countries to view the challenge to the liberal cyber order differently. Citing the discourse on decolonisation during negotiations for the UN Convention on the Law of the Sea (UNCLOS), postcolonial countries may wish to enforce sovereign borders in cybersecurity governance and therefore diverge from former colonial powers.

For example, the participant argued that India's true position on the UN Convention on Cybercrime, information and cyberspace more closely resembles the Russian position than that of the United States. The ensuing discussion included mention that the liberal cyber order itself has colonial underpinnings. India's notions of sovereignty can extend far beyond that of many Western countries, as seen through its own failed proposal to grant states ownership and control of their citizens' data stored abroad.

## Big Questions for a Rapidly Changing World Order

Expanding the discussion further, participants enquired about the structure and uncertain future of the global cyber order. A participant questioned whether the proposals represented a true order-level challenge if they have received only limited support. In response, participants called attention to the diffusion of support given many different proposals. Despite different ideas of 'cyber sov-

ereignty', many countries such as India may also be reluctant to agree to reconfigure an order from which they have benefited. The discussion highlighted that while developing countries had been involved in putting together the convention, few had ownership in the proposal-making process.

The impact of the UN Convention on common citizens was noted by another participant. The speakers highlighted that this convention, unlike previous ones, penalises any cybercrime which is an offense against the state. Referring to the earlier discussion of anti-colonial legal notions, one participant noted that this provision echoes India's law on sedition, which it inherited from its colonial legal tradition. If a person is charged with sedition, the UN convention gives jurisdiction to the state's domestic legal system to prosecute that person.

Participants also called attention to changes in the domestic politics of the United States and asked whether they are now more or less likely to sign the convention. Some argued that the United States is more likely to oppose Russia and China's proposals given greater autonomy of the U.S. private sector and greater scepticism of government under the Trump administration.

The discussion included questions about whether the convention can be considered legally binding over sovereign states at all. Participants questioned if Russia and China would truly change the nature of cybersecurity governance or simply privilege themselves the same way Western actors are privileged under the existing order.

Participants also questioned to what extent India supports the challenge to the liberal cyber order and to what extent India hedges to avoid reputation costs, especially with the United States and European Union. Relatedly, participants asked how much India's alignment or unalignment can be attributed to regime type.

Finally, a set of open questions left opportunities for further research and discussion. For one, how might policymakers in India be made aware of how the liberal cyber order has benefitted them? If Russia and China used their proposals as signalling, where might they next attempt to post a systemic challenge to international governance?

*All content reflects the individual views of the participants. The Centre for Social and Economic Progress (CSEP) does not hold an institutional view on any subject.*

*This summary was prepared by **Aleksandr Kuzmenchuk** Research Intern, CSEP  
For queries, please contact **Gurmeet Kaur**, Events Manager, CSEP at [GKaur@csep.org](mailto:GKaur@csep.org).*

**Centre for Social and Economic Progress (CSEP)**

6, Second Floor, Dr. Jose P. Rizal Marg, Chanakyapuri, New Delhi, India



Centre for Social and  
Economic Progress



@CSEP\_Org



Centre for Social  
and Economic  
Progress



[www.csep.org](http://www.csep.org)