

Cyber norms: For ensuring and open, interoperable & trusted internet

The borderless nature of the Internet from which everyone has benefitted is resulting in complex issues related to cybersecurity, jurisdiction, stability, and trust over the Internet.

The rise in hate speech, misinformation, cybercrime, ransomware attacks and state sponsored attacks highlights the need to urgently manage, address and mitigate these threats. This requires cooperation between all stakeholders.

To build Trust on the Internet and ensure the Internet is stable and secure for all, in recent years Cybernorms has been recognised as the most suitable tool for guiding state behaviour in cyberspace. However, there is a need to have defined cyber norms, voluntary standards, guidelines, best practices to manage cybersecurity-related risks and foster collaboration between countries, institutions, and stakeholder groups. There is a need to define what should be the role of governments and businesses to ensure a safe cyberspace for the citizens.

There is a need to deliberate on how cyber norms should be framed to ensure the needs of nations and citizens can be addressed. This session will deliberate on the existing challenges of implementing cyber norms, suggest recommendations on how the gaps can be addressed and what role India can play for ensuring a safe, secure, and trusted cyberspace.

The session will discuss the definition of norms, highlight the challenges in implementing cyber norms, the role of different actors, the salient features of the different Cyber norms, challenges in their enforcement, suggest recommendations for addressing the challenges and discuss what role India should play in ensuring an open, interoperable, and trusted cyberspace.