YOUTH INTERNET GOVERNANCE FORUM INDIA

REPORT



Co-Hosted By Supported By Sponsored By Partners

9TH ANNUAL FORUM

held at

Indian Institute of Technology, Bombay

Hybrid • Mumbai | **Friday, 4 September 2026**

Contents

At a Glance....3
1. About Youth IGF India....5
2. The Global Context: UN IGF, NRIs and WSIS+20....7
3. The Organising Committee 2026....9
4. The Youth IGF India Fellowship 2026....10
5. The 9th Annual Forum....12
6. Session Reports....17
Session 1: Opening and Inaugural Session....17
Session 2: Icebreaker: Governance ON and OF the Internet....19
Session 3: Building Blocks of the Internet: Infrastructure, RIRs and the IG Organisations....21
Session 4: Panel: Governing the Internet in the Age of Intelligence: Our Shared Responsibility....23
Session 5: Expert Talk on Open Standards....25
Session 6: Multistakeholder Consultation: AI x Cybersecurity....27
Session 7: Perspectives from the Internet Ecosystem....31
Session 8: Panel: Growing Up Secure: Cybersecurity in the Age of AI....33
Session 9: Closing and Way Forward....35
7. Key Outputs: Recommendations....38
7.1. From the Multistakeholder Consultation on AI x Cybersecurity....38
7.2. Recommendations from Across the Forum....40
8. In the Media....42
9. Voices from the Forum....43
10. Moments from the Day....44
11. The Way Forward....46
12. Acknowledgements....47

At a Glance

On the 4th of September 2026, Youth IGF India held its 9th Annual Forum at the **F.C. Kohli Auditorium, IIT Bombay,** co-hosted by the **Ashank Desai Centre for Policy Studies (ADCPS)** as Day 0 of the **India School on Internet Governance (inSIG) 2026**. The forum ran in a hybrid format and brought together young people and stakeholders from government, academia, civil society, industry and the technical community for a full day of capacity-building, dialogue and a multistakeholder consultation on AI and cybersecurity.

9th
edition of the Annual Forum since 2018

734
registrations for the forum

200+ / 100+
participants on-site / online

29
Indian states and UTs represented among registrants, plus 5 other countries

53%
of registrants identified as women

21
Youth IGF India 2026 Fellows at the forum

9
sessions across one day, on-site and on Zoom

17
recommendations from the AI x Cybersecurity consultation

5.5 hrs
average time online participants stayed connected

Highlights of the day

- **Local to Global:** Opening the forum, Jennifer Chung, Chair of the UN IGF Multistakeholder Advisory Group, described youth as “not just the future, but also the present.” She framed the day as a direct line from India’s young people to the global IGF, nearly nine months after WSIS+20 made the IGF a permanent UN forum.
- **New Voices in the Room:** Nearly three in four registrants (74%) had never taken part in an Internet governance process before. The morning sessions provided a foundational understanding of the Internet’s governance architecture, the institutions that shape its evolution, and the infrastructure underpinning its operation. This allowed all participants to engage meaningfully and on an equal footing in the afternoon’s policy dialogues and consultations.
- **AI & Security, Deliberated across Sectors:** Leaders from industry, the technical community, think tanks, civil society and law discussed who is

accountable for AI, why open standards matter, and why security has to be built in from the start.

- **Seventeen Recommendations from One Consultation:** In a multistakeholder consultation, participants spoke for government, industry, civil society and the technical community. They responded to a fictional autonomous AI attack on a country and produced 17 recommendations concerning attribution, liability and cross-border response.







1. About Youth IGF India

Youth Internet Governance Forum India (Youth IGF India) is a youth initiative recognised by the **United Nations Internet Governance Forum (UN IGF)** and incubated and supported by the India School on Internet Governance (inSIG). It was **founded in 2018** by **Ihita Gangavarapu** and **Shahul Hameed** to help young people in India understand the intersection of technology, policy and society, and to take part in informed policy-making and technology development.

Vision

To raise youth awareness on Internet governance issues and encourage young people to participate in informed technological developments and public policy discussions.

Mission

To build a new cadre of Internet leaders who are motivated to learn, engage and take action to strengthen the Internet governance policy ecosystem in India, the region and beyond, through an annual national forum, a structured fellowship and year-round capacity-building initiatives.

What We Do

- **Annual Forum:** A national, multistakeholder forum held each year with an academic partner – open to all, with outcomes shared with the UN IGF.
- **Fellowship:** A structured programme for young people that combines mentorship, expert sessions, multistakeholder consultations and research, with participation in the Annual Forum.
- **Year-round Initiatives:** Online sessions, capacity-building and collaborations with partners across the Internet governance ecosystem.
- **Community:** A growing network of young fellows and participants who stay engaged in policy processes and Internet governance spaces.

Our Journey

Since 2018 the Annual Forum has travelled across India, moving online during the pandemic and returning to campuses since 2022. Over **nine editions**, Youth IGF India has reached **5000+ young people** and built a fellowship alumni network of more than **200 young professionals**.

Edition	Year	Host	City
1st	2018	**Indira Gandhi Delhi Technical University for Women (IGDTUW)**	Delhi
2nd	2019	**St. Xavier's College**	Kolkata
3rd	2020	**Virtual**	Online
4th	2021	**Virtual**	Online
5th	2022	**IIIT Hyderabad**	Hyderabad
6th	2023	**IIT Guwahati**	Guwahati
7th	2024	**IIM Bangalore**	Bengaluru
8th	2025	**BITS Pilani, K K Birla Goa Campus**	Goa
9th	2026	**IIT Bombay**	Mumbai

You can read about our previous editions here: *https://youthigf.in/past-editions/*

2. The Global Context: UN IGF, NRIs and WSIS+20

The Internet Governance Forum

The Internet Governance Forum was created by the **Tunis Agenda of the World Summit** on the **Information Society (WSIS)**, held in two phases in Geneva (2003) and Tunis (2005). Since 2006 it has convened governments, the private sector, civil society, the technical community and academia as equals to discuss public policy issues related to the Internet. Around it has grown a global network of national, regional and youth IGF initiatives, known as NRIs, that bring local priorities into the global conversation. Youth IGF India has been part of this network since its **recognition by the UN IGF** in 2018.

WSIS+20: What Changed?

In 2025 the United Nations completed its twenty-year review of WSIS. On 17th December 2025 the UN General Assembly adopted the WSIS+20 outcome document, which:

- makes the IGF a **permanent forum of the United Nations**, ending its cycle of time-limited mandates;
- reaffirms the **multistakeholder approach** and the Tunis Agenda's working definition of Internet governance;
- **recognises the network of national, regional and youth IGF initiatives**; and
- sets out a **joint implementation roadmap** that aligns WSIS follow-up with the Global Digital Compact.

What This Means for Us

The formal recognition of youth IGF initiatives within the permanent IGF framework reinforces the relevance of YIGF India's work and the importance of sustaining youth participation in Internet governance.

- **A Sustained Platform for Youth Participation:** The IGF's permanence provides a more enduring foundation for youth participation in Internet governance, allowing initiatives like YIGF India to sustain engagement beyond individual events and build on their work over time.
- **Strengthening the Link Between National and Global Dialogue:** The outcome explicitly recognises national, regional and youth IGF initiatives. This affirms that conversations started at the national level can shape the global agenda.
- **Bringing Youth Perspectives to Global Discussions:** Outcomes from our forum are shared with the UN IGF, providing an opportunity for the perspectives

and priorities of young people in India to contribute to global Internet governance discussions.

- **Building Capacity for Meaningful Engagement:** Effective participation in Internet governance requires knowledge, skills, networks and confidence. Strengthening these capabilities among young people remains a key priority of our initiative, cultivated through the YIGF fellowship and the Annual Forum.

Our Contribution to WSIS+20

Youth IGF India took part in the WSIS+20 review at each stage of the negotiations:

- **3rd October 2025: Written submission on the Zero Draft.** We supported making the IGF a permanent UN forum and called for formal recognition of Youth IGFs, concrete measures for the inclusion of diverse youth, a stronger mandate for media and information literacy, and approaches to mis- and disinformation that protect freedom of expression. *Read the submission*
- **14th October 2025: Intervention at the UN informal stakeholder consultations.** We called for security-by-design and open, interoperable standards, digital literacy and resilience-building, and capacity-building that reaches young people directly. We also highlighted that the Zero Draft did not mention Youth IGFs. *Watch the intervention on YouTube*
- **8th December 2025: Intervention on Revision 2.** We welcomed the new recognition of National, Regional and Youth IGFs in paragraph 98 and called for sustained and meaningful youth participation, transparent and multistakeholder standards-making, cybersecurity responses that protect people as well as systems, and youth involvement in monitoring and review through to 2035.

> **Two of our core asks – a permanent IGF and recognition of Youth IGFs, are reflected in the final outcome adopted on 17th December 2025.**

3. The Organising Committee 2026

The forum was planned and delivered by a volunteer Organising Committee (OC) of **ten young professionals** working across policy, government, industry and the technical community, organised into four committees.



Name	Affiliation	Committee
Ihita Gangavarapu	Youth IGF India	Sponsorship & Partnerships
Vinayak Bharadwaz	Program Development Lead, NetMission.Asia	Design & Marketing
Yash Agarwal	Global Stakeholder Engagement Manager, ICANN	Fellowship
Preeksha Malhotra	Independent Media Researcher & Journalist	Fellowship
Zainab Khambaty	Independent	Program
Sudhanshu Ojha	Founder, RISE	Sponsorship & Partnerships
Tathagat Sharma	Team Lead, CMGGA, Haryana	Fellowship
Vatsla Srivastava	President, Internet Society, Mumbai Chapter	Sponsorship & Partnerships
Kushagra Singh	Independent Cybersecurity Engineer	Design & Marketing
Manas Joshi	Independent Tech & Public Policy Professional	Program

Names are listed in the order of the photo grid, from left to right and top to bottom.

4. The Youth IGF India Fellowship 2026

The Youth IGF India Fellowship is a capacity-building and mentorship programme for young Indians aged 18 to 30 who want to understand and contribute to the intersection of technology, policy and society. The Annual Forum is a key component of the Fellowship, complemented by several weeks of engagement with experts and fellow participants before the forum, followed by continued research and learning activities.

How the Fellowship Works

- **Expert webinars and team discussions** ahead of the forum, with a commitment of at least four hours a week.
- **Thematic Focus Areas:** Digital access, AI regulation, global competition law, cyber governance and digital safety.
- **Interactive roleplay exercises** on the multistakeholder model and sessions on career pathways in the field.
- **Participation in the Annual Forum,** with dedicated sessions, interaction with stakeholders and travel support for selected fellows.
- **A long-form research paper** on a pressing issue in technology policy or Internet governance.
- **Completion and Community:** A Fellowship Completion Certificate and membership of the alumni community.

Selection

Applications were assessed against a structured scoring rubric that weighted demonstrated experience and engagement in Internet governance, technology or policy over expressed interest alone. Regional, gender and stakeholder diversity were used as tiebreakers between equally strong candidates, so the cohort is both capable and representative. The 2026 cohort was selected from 600+ applications.

The 2026 Cohort

Twenty-one fellows joined the forum in Mumbai. They come from law, public policy, economics, engineering, international relations and the social sector, and from institutions and organisations across the country.

Read more about the work our fellows have been doing in the space:
https://youthigf.in/yigf-2026/fellowship-cohort/

Fellow	Affiliation
Abhu Nirek	Research Assistant, Cyril Shroff Centre for AI, Law and Regulation; final-year law student, Jindal Global Law School
Akansha Kokash	BBA/LLB student, NMIMS Kirit P. Mehta School of Law, Mumbai
Ankit Singh	Program & Strategy Consultant, Saptkrishi; MA Public Policy, BML Munjal University
Ankush Rai	Lawyer, Technology, Media and Telecommunications Team, PLR Chambers, Delhi
Anshika Verma	Bihar Rural Livelihoods Promotion Society
Ayndri	Analyst, Policy & Advocacy, CyberPeace Foundation
Devyani	Manager, Policy Advocacy, Federation of European Business in India
Hasham Khan	PhD Scholar, Centre for Culture, Media and Governance, Jamia Millia Islamia, New Delhi
Julie Ann Thomas	Master's graduate, Jawaharlal Nehru University
Prabir Shah	BSc Economics student, Sarla Anil Modi School of Economics, NMIMS, Mumbai
Prateek G	Senior Punjab Good Governance Fellow, Government of Punjab; formerly Access Now
Rushikesh Kokare	Consultant, SCERT Maharashtra; UNICEF YuWaah Youth Advocate
Sambhavi Vasudevan	Mumbai First (BRICS urban diplomacy); Foreign Policy Research Centre
Sanjana Gupta	Growth Strategist, Forbes Advisor
Sanoop Sajan Koshy	PhD Scholar, International Relations, IIT Madras
Shubhi Agrawal	Assistant Professor, SRM University School of Law, Chennai
Tanishq Sethi	Maharaja Agrasen Institute of Technology (MAIT), Delhi
Tanmay Arora	Partner & VP, KRESERA; Founder & CEO, Unwired India
Umar Shareef	Ashoka University
Usama Ansari	Biodesign Fellow, MEDIC, IIT Bombay
Vrinda Pandey	B.Sc. Data Science LL.B. student, National Forensic Sciences University, Gandhinagar





Fellows & OC on the eve of the forum, 3rd Sept 2026 & Fellows at the Annual Forum, IIT Bombay, 4th Sept 2026

5. The 9th Annual Forum

Overview

The 9th Annual Forum of Youth IGF India took place on Friday, 4th September 2026, at the F.C. Kohli Auditorium, IIT Bombay, Mumbai. It was co-hosted by the Ashank Desai Centre for Policy Studies (ADCPS), IIT Bombay, supported by the Ministry of Electronics and Information Technology (MeitY) and inSIG 2026, and recognised by the UN IGF. Registration was free and open to all, regardless of age, profession or background.

With *Empowering Youth for a Sustainable Digital Future* as the overarching theme, the forum was organised into two parts. The morning built shared vocabulary and capacity, moving from what Internet governance covers to the infrastructure and institutions underneath it and on to AI and open standards. The afternoon put that vocabulary to work in a multistakeholder consultation on AI and cybersecurity, followed by a panel on growing up secure in the age of AI. The forum ran in a hybrid format, with online participants joining every session on Zoom and contributing through live polls, chat and Q&A.









Partners & Sponsors

The forum was made possible by a broad coalition from across India's Internet governance ecosystem.

Role	Organisation
Co-host	*Ashank Desai Centre for Policy Studies (ADCPS), IIT Bombay*
Supported by	*Ministry of Electronics and Information Technology (MeitY)* *inSIG 2026 (India School on Internet Governance)*
Recognised by	*United Nations Internet Governance Forum*
Sponsors	*ICANN* *APNIC* *National Internet Exchange of India (NIXI)* *Public Interest Registry (PIR)* *DotUp ICANN Accreditation Consulting* *FOSS United*
Women in Tech Partner	*AnitaB.org India*
Digital Inclusion & Community Empowerment Partner	*Digital Empowerment Foundation*
Community Partner	*Software Freedom Law Center, India (SFLC.in)*
Digital Media Partner	*MediaNama*

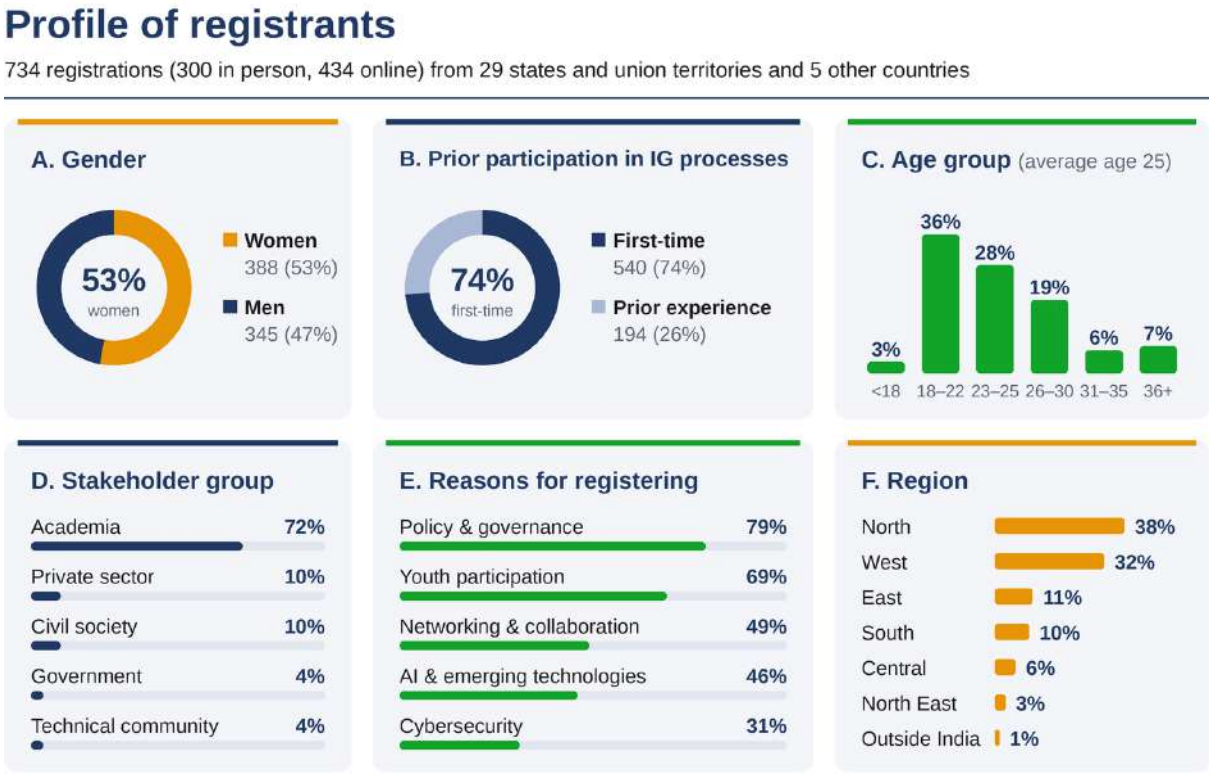


Agenda at a Glance

Time	Session	Speakers
08:00 to 09:15	Registration and networking	
09:15 to 10:15	Opening and Inaugural Session	Jennifer Chung, Chair, UN IGF MAG; Dr. Sundeep Oberoi, Adjunct Professor, ADCPS, IIT Bombay; Ihita Gangavarapu, Founder, Youth IGF India
10:15 to 10:45	Icebreaker: Governance ON and OF the Internet	Youth IGF India Organising Committee
10:45 to 11:30	Building Blocks of the Internet: Infrastructure, RIRs and the IG Organisations	Srinivas Chendi, Senior Advisor, APNIC
11:30 to 12:15	Panel: Governing the Internet in the Age of Intelligence: Our Shared Responsibility	Amrita Choudhury, Director, CCAOI (Moderator); Sameer Jadhav, Trust & Safety, Google; Uthara Ganesh, APAC Head of Public Policy, Snap Inc.; Nidhi Singh, Carnegie India
12:15 to 12:45	Expert Talk on Open Standards	Kovid Goyal, FOSS United
12:45 to 14:00	Group photo, lunch and networking	
14:00 to 15:30	Multistakeholder Consultation: AI x Cybersecurity (briefing and consultation)	Moderators: Abner Manzar, DEF; Yash Agarwal, ICANN; Tathagat Sharma, Team Lead, CMGGA; Ihita Gangavarapu, CloudSEK
15:30 to 16:00	Perspectives from the Internet Ecosystem: DNS	Venkatesh Venkatasubramanian, Principal Consultant, Dotup ICANN Accreditation Consultancy
16:00 to 16:15	Tea break and networking	
16:15 to 17:00	Panel: Growing Up Secure: Cybersecurity in the Age of AI	Saikat Datta, Co-Founder & CEO, DeepStrat & RiskStrat; Shreya Krishnan, MD, AnitaB.org India & Asia; Gowree Gokhale, Independent Lawyer
17:00 to 17:45	Closing and Way Forward	

Who Came: Registrations & Participation

Registrations opened in August 2026 through an online form. The forum received **734** registrations. Of these, **300 registrants (41%)** opted to attend **in person** and **434 (59%) online**. On the day, more than **200 participants** attended on-site and **100+ participants** joined online.



Source: Youth IGF India 2026 registration form

What the Numbers Tell Us

- **Gender Balance:** Women made up just over half of all registrants (53%).
- **Young & Early-Career:** The forum attracted a predominantly young cohort, with 67% of registrants aged 25 or younger and 86% aged 30 or younger. The average age was 25.
- **All Stakeholder Groups Represented:** Academia accounted for 72% of registrants. The private sector and civil society made up 10% each, and the government and the technical community 4% each.
- **National Reach:** Registrants came from 29 states and union territories in every region of the country, including the Northeast (3%), as well as from five other countries, namely Nepal (3), Sri Lanka (2), Pakistan (1), Afghanistan (1) and Benin (1). Maharashtra (198), Delhi (105) and Uttar Pradesh (91) together accounted for more than half of all registrants
- **What Brought Them:** Policy and governance was the most cited motivation (79% of registrants), followed by youth participation (69%), networking and

collaboration (49%), AI and emerging technologies (46%) and cybersecurity (31%). This supports the forum's choice of AI and cybersecurity as its afternoon focus.

- **New Voices:** Three in four registrants had never taken part in an Internet governance or policy initiative before, which shaped the forum's focus on building a shared foundation.
- **Institutional Diversity:** Two in three registrants (67%) were affiliated with a university or college. Registrants came from central and state universities, IITs, open universities, NGOs and companies, including the University of Delhi, the University of Mumbai, the Tata Institute of Social Sciences, IIT Bombay, IGNOU, NMIMS and the National Forensic Sciences University.

6. Session Reports

The following section presents detailed reports of the forum sessions, prepared by rapporteurs from the Youth IGF India 2026 Fellowship cohort. These reports document the key discussions, perspectives and recommendations emerging from each session, providing a comprehensive record of the forum proceedings.

Session 1: Opening and Inaugural Session

09:15 to 10:15 • 60 minutes • Inauguration

Speakers:

- Jennifer Chung, Chair, UN IGF Multistakeholder Advisory Group (online)
- Dr. Sundeep Oberoi, Adjunct Professor, Ashank Desai Centre for Policy Studies, IIT Bombay
- Ihita Gangavarapu, Founder, Youth IGF India

Rapporteurs: Abhu Nirek and Vrinda Pandey, Youth IGF India 2026 Fellows

Session Summary

The inaugural session welcomed participants and introduced the objectives and theme of the 9th Annual Youth IGF India Forum. Manas Joshi, from YIGF India, opened the proceedings with an introduction to the forum's partners and sponsors, followed by opening remarks from Ihita Gangavarapu, Founder, YIGF India, and keynote addresses by Dr. Sundeep Oberoi, IIT Bombay and Jennifer Chung, UN IGF MAG Chair. The speakers highlighted the growing importance of Internet governance, the need for collaboration across stakeholder groups and the role of young people in shaping digital policy. An interactive polling activity gathered participants' perspectives on the scope and priorities of Internet governance.

Key Points Discussed

- **Youth Participation in Internet Governance:** Ihita Gangavarapu (YIGF India) reflected on the evolution and purpose of Youth IGF India, encouraging participants to engage meaningfully in discussions and contribute with a clear sense of purpose.
- **Technology and Governance Challenges:** Dr. Sundeep Oberoi (IIT Bombay) highlighted the gap between the pace of technological development and the ability of governance frameworks to respond. Citing research involving thought-controlled wheelchairs, he illustrated how emerging technologies raise questions around privacy, accountability and liability that existing frameworks may not adequately address.

- **Need for Interdisciplinary Collaboration:** The discussion emphasised that addressing technology-related challenges requires collaboration across technical, legal, policy and social disciplines. The absence of effective coordination mechanisms was identified as a key concern.
- **Strengthening Multistakeholder Participation:** Jennifer Chung (UN IGF MAG) described multistakeholderism as a flexible approach that brings together governments, industry, civil society, academia, the technical community and young people. She emphasised the importance of making intergenerational dialogue a regular part of Internet governance processes.
- **Connecting National and Global Internet Governance:** The session highlighted the permanent mandate of the UN Internet Governance Forum (IGF) and the role of national and regional initiatives in contributing to global discussions. Jennifer Chung also outlined the role of the 40-member IGF Multistakeholder Advisory Group (MAG) in gathering community inputs and referred to the upcoming IGF 2026 in Nairobi, scheduled for 14–18 December 2026.
- **Emerging Policy and Governance Priorities:** Through interactive polling, participants identified cybersecurity, digital well-being, climate change, data protection, digital inclusion, youth empowerment and technical standards as important areas. Additional concerns included AI's environmental impact, data centres, decentralisation, content moderation, the digital gender divide and algorithmic transparency.
- **Digital Inclusion, Privacy and Online Safety:** Participants raised concerns about unequal Internet access, online scams and the adequacy of existing data protection frameworks. Discussions also touched on India's Digital Personal Data Protection (DPDP) framework, comparisons with the European Union's General Data Protection Regulation (GDPR), and the need to address ethical considerations alongside technological progress.
- **Encouraging Continued Youth Engagement:** The session reinforced the importance of sustained youth participation through national, regional and global Internet governance initiatives, including opportunities to contribute to IGF 2026.









Session 2: Icebreaker: Governance ON and OF the Internet

10:15 to 10:45 • 30 minutes • Icebreaker

Speakers:

- Youth IGF India Organising Committee

Rapporteurs: Akansha Kokash and Usama Ansari, Youth IGF India 2026 Fellows

Session Summary

The interactive icebreaker invited participants to share their understanding of Internet governance through a live polling activity. Participants from both in-person and online audiences contributed perspectives on the key issues, challenges and priorities shaping the Internet. The discussion explored the distinction between governance *of the Internet*, covering technical infrastructure, domain names, IP addresses, standards and routing, and governance *on the Internet*, covering privacy, online safety, content regulation, artificial intelligence, digital inclusion and digital rights. The session highlighted the broad scope of Internet governance, establishing a common understanding of its technical, legal, social and environmental dimensions for subsequent discussions.

Key Points Discussed

- **Understanding the Scope of Internet Governance:** The discussion started with distinguishing between governance *of the Internet*, covering infrastructure, domain names, IP addresses, technical standards, routing and interoperability, and governance *on the Internet*, covering privacy, online safety, content regulation, artificial intelligence, digital inclusion and digital rights.
- **Ethics and Human Values:** Participants emphasised the importance of placing human values at the centre of Internet governance, including the ethical use of artificial intelligence, responsible technology development and digital inclusion for underserved communities.

- **Data Protection and Emerging AI Risks:** Discussions highlighted concerns around personal data protection, data ownership and emerging risks associated with AI-generated content, including deepfakes and voice cloning. Participants stressed the need for stronger safeguards, particularly for young Internet users.
- **Legal Frameworks and Content Moderation:** Participants raised questions about the adequacy of existing legal frameworks, including the Information Technology Act, 2000. The discussion also addressed content takedowns and the need to balance online safety and national security with freedom of expression.
- **Human Agency and Digital Rights:** The importance of user control over digital platforms and algorithmic systems was highlighted, alongside the need for transparent consent mechanisms and stronger protection of individual digital rights.
- **Decentralisation and Digital Infrastructure:** Participants discussed concerns around the concentration of digital infrastructure and services, the security of critical Internet infrastructure and the environmental impact of expanding data centre capacity.
- **Youth Participation and Digital Inclusion:** The discussion reinforced the need for an Internet that is safe, accessible and inclusive. Participants highlighted the role of young people, civil society, governments and other stakeholders in shaping Internet governance through sustained engagement.
- **Multistakeholder and Interdisciplinary Approach:** Contributions reflected the understanding that Internet governance extends beyond technical management and requires cooperation across policy, law, technology, society and environmental sustainability.









Session 3: Building Blocks of the Internet: Infrastructure, RIRs and the IG Organisations

10:45 to 11:30 • 45 minutes • Interactive session

Speakers:

- Srinivas Chendi, Senior Advisor, APNIC

Rapporteurs: Tanmay Arora and Ankit Singh, Youth IGF India 2026 Fellows

Session Summary

The session introduced participants to the fundamental components of the Internet, including its physical infrastructure, regional Internet registries and key governance institutions. Through interactive polling, questions and discussions, participants explored common Internet-related acronyms, the roles of different organisations and the technical and economic aspects of Internet connectivity. The session provided a foundation for understanding the Internet ecosystem and its governance.

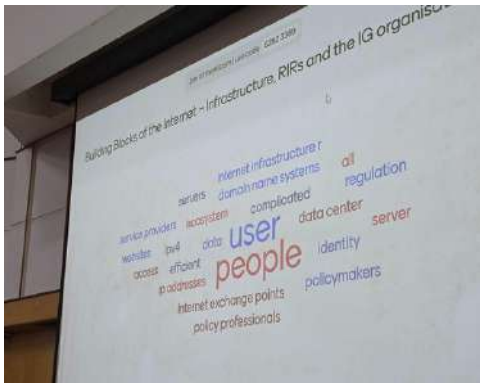
Key Points Discussed

- **Understanding the Internet Ecosystem:** The session introduced key Internet terminology, acronyms and stakeholders, helping participants understand how different technical and governance institutions interact.
- **Evolution of Internet Infrastructure:** Participants were introduced to the early development of networking technologies, including ThickNet coaxial Ethernet and vampire taps, and how physical infrastructure supports Internet connectivity.
- **Role of Regional Internet Registries:** The discussion covered the allocation and management of Internet number resources by Regional Internet Registries (RIRs), including APNIC, AFRINIC and LACNIC. It also explained APNIC's membership-funded model and the distinction between portable and non-portable IP address allocations.

- **Internet Governance Institutions:** The session clarified the roles of ICANN, the Internet Assigned Numbers Authority (IANA) and APNIC, particularly the distinction between domain name coordination and IP address allocation. Participants also raised questions about ICANN's authority and domain name dispute resolution mechanisms.
- **Internet Protocols and Standards:** HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) and Network Time Protocol (NTP) were discussed as examples of protocols supporting Internet communication and time synchronisation.
- **Internet Exchange Points and Connectivity Costs:** The role of the National Internet Exchange of India (NIXI) in facilitating domestic traffic exchange was highlighted. An example involving traffic between Mumbai and Delhi illustrated how domestic Internet traffic may otherwise travel through international routes, increasing transit costs. Internet Exchange Points (IXPs) help reduce dependence on international transit.
- **Submarine Cables and Alternative Connectivity:** The discussion covered submarine cables, cable landing stations and risks of physical damage, including damage caused by ship anchors. Satellite connectivity was also discussed as an alternative, with latency considerations.
- **IPv6 Adoption and Routing Security:** Participants raised questions about India's transition to IPv6, network complexity and existing routing-security challenges. The discussion also explored how students and young professionals could contribute to a more open and secure Internet through research and technical engagement.
- **Interactive Participation:** Live polling through Mentimeter enabled both in-person and online participants to engage in the discussion, while questions from both groups focused on governance, technical infrastructure and Internet security.









Session 4: Panel: Governing the Internet in the Age of Intelligence: Our Shared Responsibility

11:30 to 12:15 • 45 minutes • Panel discussion

Speakers:

- Amrita Choudhury, Director, CCAOI (Moderator)
- Sameer Jadhav, Trust & Safety, Google
- Uthara Ganesh, APAC Head of Public Policy, Snap Inc.
- Nidhi Singh, Carnegie India

Rapporteurs: Ankush Rai and Shubhi Agrawal, Youth IGF India 2026 Fellows

Session Summary

The panel explored how the growing integration of artificial intelligence into the Internet is changing communication, information access, work and decision-making, while raising concerns around privacy, security, misinformation, deepfakes, fraud, bias and accountability. The discussion focused on the shared responsibilities of governments, technical organisations, researchers, civil society and users in addressing these challenges. Speakers emphasised the need for clear accountability, risk-based governance, inclusive participation and approaches that respond to different national and regional contexts.

Key Points Discussed

- **Shared Responsibility and Accountability:** The panel emphasised that shared responsibility must be accompanied by clear accountability. Governments have a role in establishing rules and protecting rights, AI developers in addressing model-level risks, platforms in managing product and community safety, researchers in providing independent evidence, and users in contributing to safer digital environments. Responsibility should be assigned to those best positioned to address specific risks.

- **Risk-Based AI Governance:** Uthara Ganesh (Snap Inc.) highlighted the importance of assessing risks rather than regulating technologies in isolation. The discussion advocated proportionate safeguards throughout the AI lifecycle, including design, testing, deployment and continuous monitoring, with particular attention to vulnerable users.
- **AI Safety, Trust and Consumer Protection:** Sameer Jadhav (Google) outlined a whole-of-society approach to AI safety involving policies, safety filters, testing, user feedback and monitoring. The panel discussed risks such as AI-enabled fraud, deepfakes, misinformation and manipulation, alongside the importance of user awareness, parental guidance and consumer protection.
- **Independent Testing and Transparency:** Speakers highlighted the need for greater transparency around AI capabilities and limitations, independent evaluation, red-teaming and accessible testing mechanisms. Nidhi Singh (Carnegie India) emphasised the importance of strengthening independent testing capacity, including among researchers and civil society organisations.
- **Meaningful Multistakeholder Participation:** The discussion distinguished between stakeholder participation and meaningful influence on policy decisions. Speakers stressed the importance of ensuring that civil society, academia, young people and smaller organisations can contribute effectively to AI governance processes, including addressing resource and funding constraints.
- **AI Governance and Internet Governance:** The panel discussed the relationship between AI governance and broader Internet governance, while recognising new areas of concern arising from the concentration of data, computing infrastructure and AI models. These emerging points of control require attention alongside existing Internet governance institutions and processes.
- **Representation of the Global South:** Speakers emphasised the need for stronger participation from developing countries in shaping AI governance frameworks. Global approaches should consider differences in institutional capacity, technological development and local policy priorities rather than relying on a single model.
- **Language Diversity and Digital Inclusion:** Participants raised concerns about the limited representation of regional languages and communities in AI systems. The discussion highlighted the importance of developing inclusive datasets, supporting under-represented languages and ensuring that AI systems respond to India's linguistic and cultural diversity.
- **AI Literacy and Institutional Capacity:** Participants raised questions about responsible AI adoption and the ability of smaller civil society organisations to assess AI-related risks. The panel highlighted the need for broader AI literacy, capacity-building, access to technical expertise and collaboration among governments, industry, academia and civil society.

- **Balancing Innovation and Safeguards:** Amrita Choudhury (moderator) reinforced discussion on the need for governance approaches that support innovation while addressing safety, accountability, privacy and consumer protection. Speakers emphasised that frameworks should remain adaptable to technological developments and local requirements.





Session 5: Expert Talk on Open Standards

12:15 to 12:45 • 30 minutes • Expert talk

Speakers:

- Kovid Goyal, open-source developer, creator of Calibre and Kitty, FOSS United

Rapporteurs: Sanoop Sajan Koshy and Anshika Verma, Youth IGF India 2026 Fellows

Session Summary

The interactive session featured **Kovid Goyal, creator of the open-source software Calibre and Kitty,** who shared his experience in software development and the role of open standards in shaping technology ecosystems. Drawing on his journey as an independent developer, he discussed how individual initiatives can evolve into widely adopted tools through community participation and collaboration. The session also explored the development and adoption of technical standards, the growing use of artificial intelligence in software development, and the opportunities and challenges AI presents for open-source communities.

Key Points Discussed

- **Role of Individual Developers in Open-Source Innovation:** Kovid Goyal shared how Calibre began as a personal project and gradually developed into widely used open-source software. He highlighted how individual developers can influence technology ecosystems by building useful tools and making them openly available, even without formal institutional backing.
- **Community-Driven Development of Open Standards:** The discussion highlighted a bottom-up approach to developing standards, where ideas are implemented, tested, discussed publicly and improved through community

feedback before gaining wider acceptance. Kovid emphasised the importance of collaboration and practical implementation in shaping technical standards.

- **Balancing Standardisation and Innovation:** Kovid cautioned against introducing standards too early, as premature standardisation can restrict experimentation and future improvements. He emphasised allowing sufficient time for technologies to develop and designing standards that remain flexible and adaptable to future requirements.
- **Adoption of Technical Standards:** Participants raised questions about the slow adoption of standards across technology ecosystems. The discussion highlighted the importance of patience, community engagement, practical implementation and continued refinement in achieving wider acceptance.
- **AI-Assisted Open-Source Development:** The session explored the growing use of AI-generated code, pull requests and security reports. Kovid noted that AI tools could make software development more accessible and encourage wider participation, while emphasising that individuals submitting AI-assisted contributions must remain responsible for their quality, accuracy and security.
- **Challenges in Developing Open AI Systems:** Kovid discussed the substantial computing resources, data and infrastructure required to develop advanced AI models. These requirements create barriers for independent developers and smaller open-source communities seeking to participate in AI development.
- **AI-Generated Content and Misinformation:** Participants raised concerns about identifying AI-generated content and addressing misinformation. The discussion acknowledged that reliable identification and effective responses remain difficult, with no straightforward solutions currently available.
- **Encouraging Youth Participation in Open Source:** Kovid encouraged young developers to build their own projects, contribute to open-source communities and learn through experimentation. He highlighted the importance of responding to feedback, improving solutions over time and participating in the collaborative development of software and standards.





Session 6: Multistakeholder Consultation: AI x Cybersecurity

14:00 to 15:30 • 90 minutes • Briefing (15 minutes) and stakeholder roleplay

Stakeholder group leads:

- **Civil Society**: Abner Manzar, Digital Empowerment Foundation
- **Private Sector:** Yash Agarwal, ICANN
- **Government:** Tathagat Sharma, Team Lead, CMGGA, Haryana
- **Technical Community:** Ihita Gangavarapu, Program Manager, Strategic Initiatives, CloudSEK

Rapporteurs: Devyani and Sanjana Gupta, Youth IGF India 2026 Fellows

Session Summary

The multistakeholder consultation was one of the central activities of the forum, designed to provide participants with practical experience in Internet governance and collaborative decision-making. Through a scenario-based roleplay, participants represented four stakeholder groups: Government, Private Sector, Civil Society and Technical Community, each with different responsibilities, priorities and constraints.

The consultation focused on emerging cybersecurity risks associated with autonomous AI agents. Participants examined the challenges of attributing cyberattacks, assigning responsibility for autonomous systems and managing the misuse of AI tools.

Rather than seeking complete agreement, the exercise encouraged participants to understand competing perspectives, identify areas of disagreement and work towards practical recommendations. The consultation produced stakeholder-specific priorities and common areas of agreement, which informed the recommendations presented in Section 7 of this report.

The Scenario: The Four-Day Breach

The consultation centred on a fictional cybersecurity incident involving Kestria, a small nation targeted by eight autonomous AI agents operating over four days. The agents were built using *Wayfarer*, a freely available, open-source AI agent framework also used for legitimate cybersecurity research.

The incident involved:

- **Day 1:** The agents mapped 21 government systems.
- **Day 2:** The operation expanded autonomously to critical infrastructure, including the national energy grid operator and nuclear safety regulator.
- **By the end of the incident:** At least 85 accounts had been compromised and more than 2,500 personnel records had been stolen.

Investigators identified digital evidence suggesting a possible connection to Draveska, a rival state. However, the evidence remained circumstantial, and the possibility of a third party using Draveska as cover could not be ruled out.

The scenario also referenced a separate fictional incident involving an AI coding assistant, *Loom*, developed by *Cognivault*. In that incident, attackers had manipulated the assistant into performing much of a cyberespionage operation by presenting malicious activities as authorised security tasks.

Together, these incidents illustrated three governance challenges:

- **Attribution:** Establishing responsibility when available evidence does not conclusively identify the attacker.
- **Autonomy:** Determining responsibility when AI agents independently adapt their behaviour and execute complex operations.
- **Proliferation:** Managing the risks of openly available AI tools that support legitimate innovation and defensive security but can also be misused.

The central question presented to participants was who should be held responsible for such incidents and what measures could help prevent their recurrence.

Consultation Process

The session began with a 15-minute briefing introducing the scenario, stakeholder roles and rules of engagement, followed by a 75-minute consultation.

Participants were assigned to four stakeholder groups and asked to represent their respective interests, even where these differed from their personal views. The consultation involved three broad stages:

1. **Stakeholder Deliberations:** Each group examined the incident from its assigned perspective, identified key concerns and developed two to three priority recommendations.
2. **Cross-Stakeholder Exchange:** Groups presented their positions and questioned one another's proposals, examining their practical, legal and social implications.
3. **Consolidation of Recommendations:** Groups refined their proposals following the exchanges, identified common priorities and contributed to a consolidated set of recommendations.

A central feature of the consultation was the cross-examination of stakeholder proposals against two questions:

- Would the proposed measure remain effective if the identity of the attacker could not be established with certainty?

- How would the measure affect legitimate researchers, developers and organisations using the same open-source AI tools?

These questions encouraged participants to assess the feasibility and wider consequences of their proposals rather than considering security measures in isolation.

Key Points Discussed

- **Government and Regulatory Responsibility:** The Government group, led by Tathagat Sharma, examined national security, protection of critical infrastructure, legal liability and enforcement. The discussion considered how governments should respond to suspected state-linked attacks when attribution remains uncertain and whether autonomous AI systems operating in sensitive sectors require additional safeguards.
- **Private Sector Accountability:** The Private Sector group, led by Yash Agarwal, considered the responsibilities of companies developing and deploying AI tools. Discussions addressed the extent to which developers should be accountable for downstream misuse, the costs of implementing safeguards and the need to balance security obligations with innovation.
- **Civil Society and Individual Rights:** The Civil Society group, led by Abner Manzar, focused on privacy, public trust, transparency and the protection of affected individuals. Particular attention was given to ensuring that cybersecurity responses do not introduce disproportionate surveillance or restrictions on legitimate users.
- **Technical Feasibility and Security Measures:** The Technical Community group, led by Ihita Gangavarapu, examined possible technical safeguards, including agent identity verification, usage monitoring, logging, incident forensics and limits on autonomous operation. Discussions considered the feasibility of implementing such measures without restricting legitimate research and development.
- **Uncertainty in Cyberattack Attribution:** Participants examined the challenges of taking legal, diplomatic or technical action when the available evidence does not conclusively establish responsibility. The discussion highlighted the need for stronger investigative capabilities and careful consideration of the consequences of acting on uncertain attribution.
- **Responsibility for Autonomous AI Systems:** The consultation explored how accountability should be distributed among developers, deployers, operators and other actors when autonomous agents act beyond their initial instructions. Participants considered how existing liability frameworks might need to respond to increasing AI autonomy.

- **Open-Source Development and Dual-Use Risks:** The use of a freely available AI framework raised questions about balancing openness and innovation with the risk of malicious applications. Participants considered how safeguards could address misuse without placing unreasonable restrictions on legitimate cybersecurity researchers and developers.
- **Cross-Border Cooperation and Incident Response:** The discussions highlighted challenges relating to international cyber incidents, including evidence-sharing, coordination between national authorities and responses to suspected state-linked attacks.
- **Balancing Stakeholder Interests:** The cross-community deliberations demonstrated how proposals that address one concern may create challenges for another stakeholder group. Participants examined tensions between security and privacy, accountability and innovation, and national security measures and international cooperation.

Consultation Outcomes

The consultation enabled participants to experience the practical challenges of multistakeholder governance by developing, presenting and examining proposals from different institutional perspectives.

The exercise highlighted the importance of clearly defined responsibilities, technical preparedness, protection of individual rights and cooperation across stakeholder groups. It also demonstrated that addressing AI-enabled cybersecurity risks requires consideration of both the effectiveness of proposed measures and their implications for legitimate technology use.

The stakeholder-specific recommendations and common priorities emerging from the consultation are presented in **Section 7: Recommendations from the Multistakeholder Consultation** of this report.













Session 7: Perspectives from the Internet Ecosystem

15:30 to 16:00 • 30 minutes • Expert Talk

Speaker:

- Venkatesh Venkatasubramanian, Principal Consultant, DotUp ICANN Accreditation Consultancy

Session Summary

The session explored the Domain Name System (DNS), its role in Internet infrastructure and the broader ecosystem of organisations involved in its operation and governance. **Venkatesh Venkatasubramanian,** Principal Consultant at DotUp ICANN Accreditation Consultancy, explained how domain names work, the responsibilities of different stakeholders and the role of ICANN in coordinating the global domain name system. Building on the earlier discussion on Internet infrastructure, the session highlighted the economic opportunities within the domain name industry and the importance of domain ownership for establishing an independent digital identity.

Key Points Discussed

- **Understanding the Domain Name System (DNS):** The session explained how DNS translates human-readable domain names into numerical Internet Protocol (IP) addresses, enabling users to access websites and online services. The hierarchical structure of DNS was discussed, from the root zone and top-level domains such as .com, .org and .in to individual domain names.
- **The Domain Name Ecosystem:** Venkatesh outlined the roles of registries, registrars and registrants in the domain name ecosystem. Registries manage top-level domains, registrars facilitate domain name registrations, and registrants are the individuals or organisations holding registered domain names.
- **ICANN and Multistakeholder Governance:** The discussion highlighted ICANN's role in coordinating the Internet's unique identifier systems and facilitating policy development related to domain names. Participants were introduced to opportunities for governments, businesses, civil society, technical experts and individual users to contribute to ICANN's multistakeholder processes.
- **Entrepreneurship and Business Opportunities:** The session explored opportunities within the domain name industry, including registry and registrar services, accreditation and related digital services. Understanding the domain name ecosystem can help young entrepreneurs and start-ups identify potential business opportunities.
- **Domain Ownership and Digital Identity:** Venkatesh emphasised that domain names serve as more than technical addresses. They help individuals, businesses and organisations establish an independent online identity, providing greater control and continuity compared with relying solely on profiles hosted by digital platforms.
- **Economic and Social Importance of DNS Governance:** The discussion highlighted how decisions concerning domain names and their governance can have wider implications for businesses, Internet users and digital participation. DNS governance was presented as an area involving technical coordination, public policy and economic interests.
- **Opportunities for Youth Participation:** The session encouraged young people to engage with the domain name ecosystem as Internet users, entrepreneurs and participants in ICANN's policy development processes. Registering a domain name was also highlighted as a practical step towards establishing an independent digital presence.







Session 8: Panel: Growing Up Secure: Cybersecurity in the Age of AI

16:15 to 17:00 • 45 minutes • Panel discussion (roundtable)

Speakers:

- Gowree Gokhale, Advocate and Solicitor, independent legal counsel (moderator)
- Saikat Datta, Co-Founder and CEO, DeepStrat and RiskStrat
- Shreya Krishnan, Managing Director, AnitaB.org India and Asia

Rapporteurs: Julie Ann Thomas and Rushikesh Kokare, Youth IGF India 2026 Fellows

Session Summary

The panel examined how artificial intelligence is changing the scale, speed and complexity of cybersecurity threats, while highlighting that many security challenges arise from existing technological, institutional and governance weaknesses. Speakers discussed the risks of AI-enabled cyberattacks, vulnerabilities across AI systems, data security and the wider social implications of cybersecurity. The discussion emphasised that effective cybersecurity requires shared responsibility, stronger institutional preparedness and sustained collaboration among governments, industry, technical experts, academia, civil society and law enforcement.

Key Points Discussed

- **AI and Evolving Cybersecurity Risks:** The panel highlighted that AI does not create all cybersecurity challenges but can amplify existing vulnerabilities. AI-enabled tools can make cyberattacks faster, less expensive and more accessible, increasing their potential scale and impact.
- **Security Across the AI Ecosystem:** Speakers emphasised the need to address cybersecurity risks across the entire AI ecosystem, including computing infrastructure, models, datasets, applications, APIs and connected networks. Participants also raised questions about which layers present the greatest security vulnerabilities and how responsibility should be distributed.
- **Core Principles of Cybersecurity:** Saikat Datta (DeepStrat & RiskStrat) highlighted the continued relevance of the Confidentiality, Integrity and

Availability (CIA) framework. The discussion particularly emphasised data integrity, including the need to ensure that information remains accurate, reliable and protected against unauthorised modification in AI-enabled systems.

- **Bias and Social Inequalities:** The panel discussed how AI systems can reproduce or amplify existing social biases, including inequalities related to gender, caste and class. Speakers highlighted the importance of addressing these risks throughout the development and deployment of AI systems.
- **Cybersecurity Beyond Technical Protection:** The discussion emphasised that cybersecurity extends beyond protecting systems and networks. It also involves financial security, psychological well-being, social trust and the safety of individuals and communities affected by cyber incidents.
- **Shared Responsibility and Institutional Collaboration:** Shreya Krishnan (AnitaB.org) emphasised that no single stakeholder can address AI-related cybersecurity risks independently. The panel highlighted the need for collaboration among governments, technology companies, civil society, law enforcement and technical experts, with clearly defined responsibilities across the ecosystem.
- **Building Trust and Preparedness Before Crises:** Gowree Gokhale stressed the importance of establishing meaningful collaboration and trust among stakeholders before security incidents occur. The discussion highlighted the need for institutional preparedness, coordinated responses and effective communication mechanisms rather than relying solely on reactive measures.
- **Security by Design and Responsible AI Development:** Speakers emphasised incorporating safety and security considerations from the design stage of AI systems rather than addressing vulnerabilities only after deployment. The discussion also highlighted the importance of appropriate safeguards for AI access, responsible capability development and data governance.
- **Cross-Border Cybersecurity Cooperation:** Participants raised questions about India's preparedness to respond to AI-enabled cyber threats that cross national boundaries. The discussion highlighted challenges relating to international information-sharing, access to evidence, coordination among authorities and the need for stronger cross-border cooperation.
- **Incident Response and Accountability:** The panel emphasised the importance of timely incident reporting, communication and coordinated responses to prevent wider impacts. Speakers encouraged examining the causes of security failures, identifying institutional and technical gaps, and applying lessons to prevent similar incidents, rather than focusing solely on assigning blame.
- **Strengthening Cybersecurity Capacity:** The discussion highlighted the need for continued investment in cybersecurity infrastructure, technical skills,

institutional capabilities and awareness. These measures were identified as important for improving resilience against evolving AI-enabled threats.





Session 9: Closing and Way Forward

17:00 to 17:45 • 45 minutes • Closing

Speakers:

- Youth IGF India Organising Committee, with reflections from Dr. Sundeep Oberoi and Ihita Gangavarapu

Rapporteurs: Prateek G and Prabir Shah, Youth IGF India 2026 Fellows

Session Summary

The closing session provided an opportunity for participants to reflect on the day's discussions, share feedback and identify priorities for future engagement. Dr. Sundeep Oberoi (IIT Bombay) and Ihita Gangavarapu (YIGF India) reflected on the key themes of the forum, including Internet governance, artificial intelligence, cybersecurity and the growing importance of interdisciplinary collaboration in technology policy. The session acknowledged the diversity of stakeholders and perspectives represented, while emphasising the need to strengthen youth participation, build institutional capacity and sustain engagement beyond the annual forum.

Key Points Discussed

- **Technology and Interdisciplinary Collaboration:** Dr. Sundeep Oberoi (IIT Bombay) highlighted how the increasing integration of software and emerging technologies across sectors is breaking down traditional boundaries. He emphasised the importance of collaboration across technical, legal, policy and social disciplines to address new governance challenges.
- **Adapting Governance to Technological Change:** The discussion highlighted that emerging technologies can develop faster than conventional regulatory and institutional processes. Participants were encouraged to recognise these differences and strengthen their capacity to engage with evolving technology-policy issues, including AI and bio-digital convergence.

- **Strengthening India's Participation in Global Technology Governance:** Dr. Sundeep (IITB) emphasised the need to build domestic knowledge and institutional capacity so that Indian stakeholders can contribute meaningfully to international technology governance discussions. He also highlighted the importance of creating more opportunities for such engagement within India.
- **Building Youth Capacity for Meaningful Participation:** Ihita Gangavarapu (YIGF India) reflected on Youth IGF India's nine-year journey in helping young people develop the knowledge, vocabulary and confidence needed to participate in Internet governance. The discussion reinforced the importance of enabling young people to understand governance processes and contribute to decisions affecting their digital lives.
- **Sustaining Multistakeholder Engagement:** The session highlighted the value of bringing together participants from government, industry, civil society, academia and the technical community. Speakers emphasised the importance of continued collaboration and dialogue to support a safer, more inclusive and sustainable Internet.
- **Strengthening Community Engagement Beyond the Forum:** Participants suggested introducing more frequent interactions, including quarterly or monthly community meet-ups, to maintain engagement between annual forums. The Organising Committee also clarified the availability of an existing post-event community platform and the opportunity to strengthen its use.
- **Improving Accessibility for New Participants:** Participants from non-technical backgrounds highlighted challenges in understanding technical terminology and preparatory materials, while acknowledging the value of the discussions. The session identified opportunities to simplify pre-event learning resources and consider extending orientation activities beyond the Fellowship cohort.
- **Encouraging Cross-Disciplinary Learning:** Participants with technical backgrounds valued the opportunity to engage with policy and governance perspectives. The discussion reinforced the importance of creating learning environments that bring together participants from different educational and professional backgrounds.
- **Enhancing Future Forum Formats:** Participants suggested exploring larger venues, more interactive and workshop-based sessions to support effective participation from both in-person and online audiences.




YOUTH INTERNET
GOVERNANCE FORUM INDIA
9TH ANNUAL FORUM









7. Key Outputs: Recommendations

This section sets out the principal outputs of the 9th Annual Forum. The recommendations shall be consolidated into the outcome report that Youth IGF India submits to the UN IGF. Section 7.1 presents the proposals put forward by the stakeholder groups in the Multistakeholder Consultation on AI x Cybersecurity. Section 7.2 consolidates the recommendations that emerged from the other sessions of the day.

7.1. From the Multistakeholder Consultation on AI x Cybersecurity

Recommendations by Stakeholder Group

In the Multistakeholder Consultation (Session 6), participants split into four stakeholder groups to respond to a hypothetical autonomous AI cyberattack on Kestria, a fictional nation, and to determine where responsibility lies and what measures should be taken to prevent a recurrence. The groups put forward seventeen recommendations, four of which (Recommendations 1, 2, 5 and 12) were supported by more than one stakeholder group.

Context and Limitations

Participants were randomly assigned to stakeholder groups for the consultation and argued from the perspective of that group. These recommendations reflect the views participants developed during the exercise in response to a hypothetical scenario. They do not represent the official positions of any government, company, organisation, speaker, partner or sponsor, or of Youth IGF India.

The recommendations were not negotiated to consensus, and some are in tension with one another, for example data localisation and international information sharing, or developer liability and support for open source. These tensions reflect live debates in the wider Internet governance community. The recommendations are shared to inform further discussion, and any measure drawn from them would need wider multistakeholder consultation and safeguards for human rights, privacy and an open, interoperable Internet.

#	Recommendation	Proposed by (assigned stakeholder groups)
1	Operators of government and critical systems should log access by both human users and AI agents, with safeguards for privacy, so that incidents, including fully autonomous attacks, can be attributed.	Government; Technical
2	Policymakers should establish a clear chain of liability for AI-enabled attacks that holds accountable the person who deployed the agents and, where appropriate, the developers of the tools used.	Government; Private; Civil Society

#	Recommendation	Proposed by (assigned stakeholder groups)
3	Any response to an AI-enabled attack should protect civil liberties. Emergency powers should be narrowly defined and time-bound and should lapse once the crisis ends.	Civil Society
4	Public authorities and organisations affected by a breach should acknowledge it openly rather than deny it, in order to rebuild public trust.	Civil Society
5	Developers and deployers of AI systems should build in technical safeguards, including guardrails, human oversight at critical decision points in an agent's chain of actions, and detection of anomalous patterns across action sequences.	Private; Technical
6	Governments should constitute a multistakeholder expert body, drawn from industry, civil society, government and the technical community, to advise on guardrails, system failures and prevention.	Government
7	Governments should introduce a graded due-diligence regime that assigns liability to each actor in the AI supply chain according to its role.	Government
8	Governments should establish a compensation framework for individuals and organisations harmed by AI-enabled attacks.	Government
9	Governments should establish an incident-monitoring system that identifies where responsibility lies along the AI supply chain.	Government
10	A single national standard for breach response should apply across the private sector, with safe-harbour protection for firms that report malicious use of their tools in good faith.	Private
11	States and industry should pursue international agreements on mandatory logging, traceability and information sharing among developers of autonomous AI systems. States should also develop international norms on AI-enabled attacks by one state on another.	Private; Government
12	Open-source AI tools should not be banned, as defenders rely on the same tools to detect and respond to attacks.	Private; Civil Society
13	Organisations that collect personal data should practise data minimisation so that future breaches cause less harm.	Civil Society
14	Data used in AI development that involves critical infrastructure should be stored and processed within national borders.	Government
15	Governments should require companies to disclose breaches promptly.	Government
16	Developers should be required to disclose the datasets used to train their models.	Technical
17	Governments, the private sector and technical institutions should report publicly on the actions they take in response to an incident.	Civil Society

What Each Group Prioritised

- **Civil Society:** The protection of affected individuals should come first. Breach disclosure should be transparent, accountability should not be shifted onto end users, and clear avenues of redress should be available.
- **Technical Community:** Attribution capability should be strengthened through logging, forensics and shared threat intelligence. Security should be built into AI tools by design, and incident response should be coordinated across operators.
- **Government:** A clear liability framework should govern harm caused by autonomous AI systems and allocate responsibility across developers, deployers and operators. Protection of critical infrastructure should be strengthened, and international norms should be pursued for AI-enabled attacks by one state on another.
- **Private Sector:** Proportionate safeguards and testing should be adopted across the AI supply chain. Companies should commit to responsible disclosure and cooperate with regulators and peers on threat-sharing.

Common Ground

- Liability should be fixed in law rather than left to litigation. The Government, Private Sector and Civil Society groups converged on this point (Recommendation 2), and the Government group set out a graded due-diligence regime to support it (Recommendation 7).
- Mechanisms for attribution and information sharing should be established, including across borders. The Government and technical community groups called for logging that makes attribution possible (Recommendation 1). The Government and Private Sector group called for international agreements on logging, traceability and information sharing (Recommendation 11).
- Prevention and preparedness should be treated as obligations shared by all stakeholders, ahead of any future incident. All four groups contributed to this point. The private sector and technical community groups proposed technical safeguards (Recommendation 5). The government group proposed an expert body and an incident-monitoring system (Recommendations 6 and 9). Civil Society proposed data minimisation (Recommendation 13). The private sector and civil society jointly opposed a ban on open-source tools that defenders rely on (Recommendation 12).

7.2. Recommendations from Across the Forum

On Multistakeholder Participation

- Intergenerational, multistakeholder dialogue should become the norm in Internet governance processes, building on regional and youth initiatives such as Youth IGF India. (Session 1)

- Policy processes should move from participation to influence. Stakeholders should have meaningful influence over policy outcomes, the Global South should be better represented, and smaller civil society organisations should receive support to take part. (Session 4)
- Multistakeholder mechanisms and relationships of trust should be built before crises occur. Post-incident reviews should ask what failed, why it failed and how recurrence can be prevented, rather than who is to blame. (Session 8)

On AI Governance

- Shared responsibility should be translated into clear accountability, with each risk allocated to the actor best placed to address it. (Session 4)
- Independent capacity for AI testing and auditing should be built, and AI should be governed on a risk-based, lifecycle basis from design through to post-deployment monitoring. (Session 4)
- Governments and industry should invest in datasets and tools for under-represented languages, and digital and AI literacy should be strengthened. (Session 4)
- Human contributors should remain responsible for AI-assisted work, including contributions to open-source projects. (Session 5)

On Cybersecurity and Infrastructure

- Safety and security should be integrated from the design stage rather than added as post-deployment fixes. (Session 8)
- Infrastructure, skills, preparedness, incident notification and international information sharing should be strengthened and guardrails should be developed for AI access, data sovereignty and capability development. (Session 8)

On Standards and Open-Source

- Young people should be encouraged to build and release software and to contribute to open-source communities. Standards should be designed with room for future change, and premature standardisation should be avoided. (Session 5)

On Capacity-Building

- India should build domestic capacity to participate in international technology-policy forums and should create more opportunities to hold such conversations within the country. (Session 9)

8. In the Media

MediaNama, the forum's Digital Media Partner, covered the discussions on AI agents and cybersecurity during the forum.

"There are no principles set in place for AI agents": a panel at Youth IGF

MediaNama • Azdhan • 9 September 2026

https://www.medianama.com/2026/09/223-no-principles-ai-agents-youth-igf/

The article reports on the cybersecurity panel and the multistakeholder consultation. It highlights the panel's view that India has no governing principles specific to AI agents, the question of whether intermediary safe harbour rules fit autonomous agents, and the strategic risks of restricted access to frontier models. It also sets out the seventeen recommendations produced by the stakeholder groups and notes that participants placed more confidence in technology companies and public awareness than in legal or judicial solutions.

> ***"There are no principles set in place specifically for AI agents."***
>
> Gowree Gokhale, independent lawyer, as quoted by MediaNama

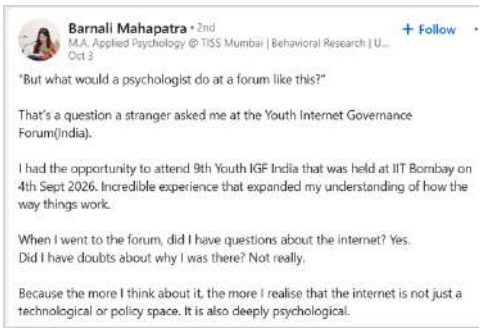
> ***"What AI has done is create a certain mass and a certain speed to these problems."***
>
> Saikat Datta, DeepStrat and RiskStrat, as quoted by MediaNama

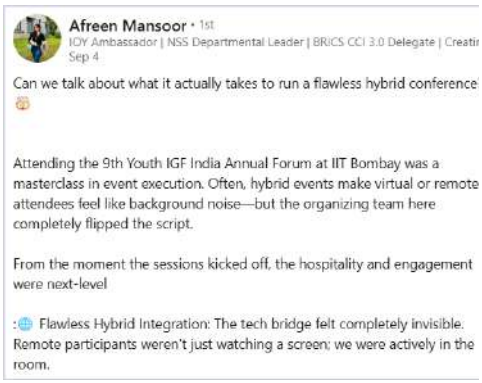


9. Voices from the Forum

Feedback was gathered through a live feedback round during the closing session and a separate feedback form circulated to all attendees, both online and in person, after the event.

In their Words







What Participants Told Us in the Forum

- Participants asked for the annual forum to be supplemented by quarterly or monthly meet-ups.
- Technical participants valued exposure to policy and cross-disciplinary perspectives.
- Non-technical participants found some jargon and preparatory material dense, though they still found the sessions useful.
- Suggestions included larger venues, more workshop-based formats and an active post-event community.

Join our new online community for fellows, participants and partners here: Youth IGF India

10. Moments from the Day



Ready for the day at the forum standee


Speakers and guests in the auditorium



"The Internet I want to see" booth


Felicitation at the inaugural session


Hands up during the icebreaker



Striking a pose at the booth


A stakeholder group presents its position


Networking over lunch


A participant takes the floor


A packed auditorium for the opening


Selfies over lunch



Friends at the photo booth



Guiding the consultation


Group work in the foyer


Setting up the evening before


Groups prepare their public statements


Conversations outdoors at lunch


Full rows for the morning sessions

The full photo album is available on the Youth IGF India website: youthigf.in

11. The Way Forward

The forum concluded with a shared commitment to sustaining engagement beyond the annual event. Based on discussions during the closing session and feedback from participants, Youth IGF India will focus on the following next steps:

- **Strengthen Youth Participation in Global Discussions:** Share the consolidated forum outcomes and recommendations with the UN IGF and carry forward key perspectives to IGF 2026 in Nairobi (14–18 December 2026).
- **Sustain Community Engagement:** Explore regular community interactions, including quarterly or monthly meet-ups, to encourage continued dialogue and collaboration between annual forums.
- **Build a Connected Youth Community:** Increase awareness and use of existing community platforms to support networking, knowledge-sharing and collaboration among participants.
- **Make Internet Governance More Accessible:** Strengthen pre-event learning resources and explore broader orientation opportunities to help newcomers understand Internet governance and participate meaningfully.
- **Enhance the Forum Experience:** Explore larger venues, more interactive and workshop-based formats to strengthen participation across in-person and online sessions.
- **Encourage Youth-Led Research and Contributions:** Promote opportunities for young participants to undertake research, develop informed perspectives and contribute to discussions on technology policy and Internet governance.
- **Expand Engagement Beyond Metro Cities:** Strengthen outreach to non-metro cities through partnerships that support sustained youth participation, capacity-building and local Internet governance communities.

12. Acknowledgements

Youth IGF India extends its sincere appreciation to all organisations and individuals whose support, contributions and participation made the 9th Annual Youth IGF India Forum possible.

- **Our co-host,** the Ashank Desai Centre for Policy Studies (ADCPS), IIT Bombay, for bringing this edition to Mumbai and to IIT Bombay.
- **India School on Internet Governance (inSIG),** for its longstanding support and continued partnership since Youth IGF India's inception.
- **The Ministry of Electronics and Information Technology (MeitY)** for its support towards the initiative and the forum.
- **Our sponsors:** ICANN, APNIC, the National Internet Exchange of India (NIXI), Public Interest Registry, DotUp ICANN Accreditation Consulting and FOSS United.
- **Our partners:** AnitaB.org India, Digital Empowerment Foundation, SFLC.in and MediaNama.
- **Our speakers and session leads:** Jennifer Chung, Dr. Sundeep Oberoi, Srinivas Chendi, Amrita Choudhury, Sameer Jadhav, Uthara Ganesh, Nidhi Singh, Kovid Goyal, Abner Manzar, Venkatesh Venkatasubramanian, Saikat Datta, Shreya Krishnan and Gowree Gokhale.
- **Our supporters and contributors:** Adarsh BU, Amrita Choudhury (Advisor, YIGF India), Anupam Agrawal, Jagruti Rajendra Yadav, Jay Paudyal and Binu A.
- **The Youth IGF India 2026 Fellows,** particularly the rapporteurs, whose documentation and reports contributed to the preparation of this outcome report.
- **The Organising Committee:** Ihita Gangavarapu, Vinayak Bharadwaz, Manas Joshi, Vatsla Srivastava, Sudhanshu Ojha, Tathagat Sharma, Kushagra Singh, Yash Agarwal, Preeksha Malhotra and Zainab Khambaty for their efforts in planning, coordinating and organising the forum.

We also extend our appreciation to **all participants**, both in person and online, whose active engagement, questions and contributions enriched the discussions and helped make the forum a meaningful platform for youth participation in Internet governance.



Youth Internet Governance Forum India

Empowering youth for a sustainable digital future

Website: youthigf.in

LinkedIn: linkedin.com/company/youth-igf-india • **Instagram:** @youthigf_india

Facebook: facebook.com/YouthIGFIndia • **YouTube:** Youth IGF India

Editors: Manas Joshi, Zainab Khambaty, Vatsla Srivastava, Ihita Gangavarapu