Synthesis Document

Asia Pacific Regional Internet Governance Forum 2025 (Virtual Conference)

The Process

This Synthesis Document aims to document key output discussions from the Asia Pacific Regional Internet Governance Forum (APrIGF) 2025, often topics of common interest and utmost relevance to Internet governance in the Asia-Pacific (APAC) region. The Synthesis Document has developed into one of the unique knowledge innovations of the APrIGF and has inspired other national and regional initiatives to build their own similar processes.

The 2025 Synthesis Document was drafted, synthesised, and published by the 2025 Drafting Committee (DC) with the assistance of the APrIGF Secretariat. Public inputs were sought during the input periods (2 cycles) as well as from the APrIGF 2025 conference Townhall sessions. Comments were collected on the platform: https://comment.aprigf.asia during the input periods.

2025 Drafting Committee

Alban Kwan (Co-Chair)
Syed Sultan Kazi (Co-Chair) (Access & Inclusion Penholder)
Yien Chyn Tan (Co-Chair) (Innovation & Emerging Technologies Penholder)
Anika Vashisth (Access & Inclusion Penholder)
Amrita Choudhury (WSIS+20 Penholder)
Joyce Chen (WSIS+20 Penholder)
Om Prakash Sharma (Resilience & Sustainability Penholder)
Shahanaj Begum (Security & Trust Penholder)
Ashirwad Tripathy
Cheryl Langdon-Orr
Dr. Amrit Chhetri
Elizabeth Pollard
Hino Samuel Jose
Nguyen Thi Ngoc Huyen
Ritu Srivastava
Sharmin Israil
Winston Roberts
Yuan-Ting Lin
Zainab Fayyaz Cheema
For the full affiliation information, please see Appendix I.

Table of Contents

The Process **2**
2025 Drafting Committee **2**
Preamble **4**
Special Track: WSIS+20 Review Process **6**
WSIS+20 Working Group & Webinars 6
APrIGF2025 8
Track 1: Access & Inclusion **11**
Digital Inclusion for All 11
AI for Justice & Public Good 21
Disconnect between Projected Internet Coverage and Real User Experiences 23
Track 2: Innovation & Emerging Technologies **26**
Inclusivity in Digital Policymaking, Particularly on Youths' Role 26
AI Governance 28
Emerging Technologies and Tools 31
Track 3: Sustainability **33**
Track 4: Security & Trust **34**
Governing Digital Public Infrastructure in the Asia-Pacific 34
The Human Dimension of Security and Trust in the Digital Age 37
Track 5: Resilience **39**
Infrastructure Resilience 39
Resilience Against Regulatory Overreach 41
Funding for Resilience 43
Annex I Regional Parliamentary Track Discussion Summary* **45**
Navigating the Net: An Introduction to the Internet Ecosystem 45
Governing Digital Platforms in the Asia-Pacific: Strengthening Public Policy through Multistakeholder Insights 46
Appendix I 49

**report received from the IGF Secretariat*

Preamble

The Asia Pacific Regional Internet Governance Forum (APrIGF) 2025 was held virtually from **11–14 October 2025**, hosted by the Internet Governance Institute (IGI) and executed by the APrIGF Multi-Stakeholder Group (MSG) in collaboration with the APrIGF Secretariat.

This year also marks a significant milestone in the history of Internet governance, as it is the 20th anniversary of the World Summit on the Information Society (WSIS), first convened in Geneva in 2003. The Internet Governance Forum (IGF)—of which APrIGF forms a regional component—was established as an outcome of the WSIS Tunis Summit in 2005. The IGF and WSIS are therefore deeply interconnected, and so is APrIGF. The WSIS+20 review will be a critical moment for setting the vision of the Information Society, as well as a roadmap for Internet Governance, for the next decade and beyond. As such, APrIGF 2025 convened a WSIS+20 Working Group (WG), with WG members driving outreach and discussions on the topic with the regional community. The 2025 Synthesis Document includes a dedicated segment covering the key discussion outputs from engagement efforts (e.g. webinars) and the APrIGF community's perspectives on the WSIS+20 review.

Against this backdrop, APrIGF 2025 focused on the overarching theme: **"The Future of Multistakeholder Digital Governance in Asia Pacific."** The emphasis on "multistakeholder" reflects its foundational role in shaping both the **governance *of*** the Internet (its infrastructure and technical functioning) and **governance *on*** the Internet (the issues arising from its use). As emerging challenges such as artificial intelligence (AI), digital safety and security, geo-political challenges, and safeguarding Internet infrastructure, newer forms of digital divide, and meaningful youth participation have come to the forefront, strengthening multistakeholder approaches remains essential.

The overarching theme also highlights the concept of "Digital Governance," acknowledging that the outcomes of the WSIS+20 Review will intersect with the United Nations' Global Digital Compact (GDC). This underscores the importance of IGF processes, including their national, sub-regional, regional, and youth initiatives (NRIs)--such as APrIGF—in shaping global digital policies. To reflect the breadth of Internet and digital governance, APrIGF 2025 featured the following five high-level thematic tracks. These tracks ensured that APrIGF 2025 provides space

for a wide-ranging and inclusive discussion of the key issues shaping the future of digital governance in the Asia-Pacific (APAC) region.

1. Access & Inclusion
2. Innovation & Emerging Technologies
3. Sustainability
4. Security & Trust
5. Resilience

APrIGF 2025 also featured a dedicated parliamentary track to strengthen participation of Parliamentarians from the APAC region in discussions relating to the use, evolution, governance of the Internet, and related digital policy and technologies. Summary of discussions is available under Annex I below.

Additionally, the Asia Pacific Youth IGF (yIGF) was held in parallel as a sister event to the APrIGF, emphasising youth engagement as co-governors within the multistakeholder framework.

Special Track: WSIS+20 Review Process

WSIS+20 Working Group & Webinars

In line with the World Summit on the Information Society 20-year Review Process (WSIS+20) this year, the Asia Pacific Internet Governance Forum (APrIGF) community convened a WSIS+20 Working Group (WG), focusing on discussions and engagements on issues relevant to the APAC Region. In addition to fortnightly WG calls attended by WG members, a key highlight from this effort was the two webinars conducted before the APrIGF 2025 to raise awareness and engage with the wider Asia Pacific (APAC) stakeholders on this process. To continue engaging on this topic, a third webinar was further held after the APrIGF 2025.

The WSIS+20 WG will continue its efforts throughout 2025, exploring additional regional outreach as required, in line with the preparatory process roadmap.

Webinar 1

The first webinar (Webinar 1) was conducted on Tuesday, 3 June 2025, from 06:00-07:15 UTC, focusing on raising awareness of the WSIS+20 Review Process. The webinar invited several speakers from various stakeholder groups, including government, civil society, and the technical community, who shared an overview of the WSIS+20, and what it means for the regional community, and key considerations for the review process.

Webinar 2

The second webinar (Webinar 2) was held on Wednesday, 17 September 2025, from 05:00-06:30 UTC. This interactive session divided the attendees into breakout groups for detailed discussion on five main sections of the WSIS+20 Zero Draft. The five sections were:

- Multistakeholder Model of Internet Governance
- Digital Access, Inclusion & Connectivity
- Human Rights
- Building Confidence and Security in Information and Communication Technologies (ICTs)
- Digital Economy

To highlight, a written input document based on key discussion points from Webinar 2 was submitted to the WSIS+20 Review Process co-facilitators, offering collective input from the APrIGF community for consideration. The full input document is available for reference.

As a summary from Webinar 2, participants stressed the importance of retaining the multistakeholder model while addressing power imbalances, funding gaps, and improving local participation. They advocated for stronger measures to bridge various digital divides, including those related to affordability, multilingual content, and resilience against geopolitical and environmental challenges. The human rights section was commended but was noted as lacking actionable solutions, particularly on online harms and gender-based issues. For ICT security, participants emphasised the need for clear definitions, practical risk mitigation frameworks, and a balance between privacy and harm prevention. Finally, the digital economy discussion called for clarity on equitable participation, addressing market concentration, and ensuring inclusion of vulnerable groups in digital financial systems.

Webinar 3

The third webinar (Webinar 3) took place on Monday, 17 November 2025, from 03:00-04:00 UTC, focusing on the revised draft outcome document (Revision 1). Speakers from the government, Informal Multistakeholder Sounding Board (IMSB) and technical community were invited to provide an update on the WSIS+20 Review process and insights as to how the negotiations are shaping up, including key focus areas or areas of concern, analysis of the Revision 1 outcome document against the WSIS+20 Zero Draft, highlighting text that have been strengthened or softened, and outlining issues to be considered in the next version. A 30-minute Open Mic session was dedicated in this webinar as the session aimed to engage the Asia Pacific community in an open dialogue to provide feedback and inputs on possible text revision on Revision 1.

Overall the community welcomed the text in Revision 1 especially related to closing the digital divide, with emphasis on financing mechanisms to provide meaningful connectivity, proposal to set up a task force to deliberate on future financial mechanisms for digital development, addition of the NETmundial+10 guidelines for multistakeholder collaboration, mention of youth as active stakeholders, continued support for permanency of the Internet Governance Forum (IGF)'s mandate including recognition of Youth IGF and other IGF intersessional work,

recommendation for strengthening alignment between WSIS, Global Digital Compact (GDC) and the Sustainable Development Goals (SDGs).

Concerns were raised on the softening of language related to human rights and environmental impacts. The community expressed hope to see more clarity on the roles of the United Nations Group of the Internet Society (UNGIS) and United Nations Office for Digital and Emerging Technologies (ODET) in WSIS implementation to avoid duplication, and more granularity on the financial mechanisms in the next document version.

APrIGF2025

The APrIGF community also discussed the WSIS+20 Review Process during APrIGF 2025. The main sessions covering this topic were the WSIS+20 High-Level Plenary and Townhall Session[1] attended by the United Nations (UN) WSIS+20 Co-Facilitators, as well as a session organised on 'Internet Governance (IG) at a Crossroads: Asia-Pacific Priorities for WSIS+20 and Beyond'[2].

High Level Plenary & Townhall

The APrIGF community appreciated the text in the Zero Draft reiterating the need to preserve the multistakeholder model in a way that achieves its genuine intended purpose - true opportunities for participation from all stakeholders. Reiterating support for a permanent mandate of the IGF, recognition of National, Regional, Subregional and Youth Internet Governance Forums (NRIs), the community called for avoiding fragmentation or duplication of work, and looks forward to a transparent and open review process.

The community emphasised the need for further specificity and consideration of the issue of AI governance and its impacts on international trade, human rights, and labour issues. The desire for action oriented outcomes to be produced at WSIS+20 was expressed in order to support an effective and consistent approach to AI governance.

A key concern for the WSIS+20 Review was how to address the shortcomings of the Internet in regards to global connectivity, equitable access, and support for marginalised communities, especially their labor and environmental rights. Participants expressed that these issues remain

[1] APrIGF 2025 WSIS+20 High Level Session: https://ap.rigf.asia/2025-program-schedule/#wsis20
[2] APrIGF 2025, "Internet Governance at a Crossroads: Asia-Pacific Priorities for WSIS+20 and Beyond". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2E1ZTNiZDNkYy8vMzkvLzIzOTMvLzA= (last accessed on 8 December 2025)

prevalent in modern society and noted a desire for the WSIS+20 Review to consider how to better address inequalities relating to the Internet. The community felt these issues should be a key point of focus in the coming decade to truly make progress on the goal of inclusivity and equal access.

The APAC community has a particular focus on diversity and multilingual support as key facets of achieving equal participation. The community noted the limitations of access to Internet decision making processes in the APAC region, particularly for youth, due to limited multilingual support and opportunities for participation. The importance of supporting participation and inclusion of marginalised groups and underserved communities in the decision making process, in the language of their preference, was emphasised. The continued impact of economic and social inequality on access to global connectivity was discussed, and the community noted the importance of working to close the digital divide.

It was emphasised that WSIS+20 should consider the diverse needs of stakeholders from around the world and how the Internet can be improved for all.

IG at a Crossroad: APAC Priorities for WSIS+20 and Beyond

The WSIS+20 Review Process needs to remain open and inclusive for multistakeholder participation and input to ensure meaningful global participation towards shaping a resilient digital future. The need to protect and reinforce the multistakeholder model and to encourage more inclusive participation was emphasised, along with urging the APAC community to engage in the WSIS+20 Review Process. Recognition of all stakeholder groups and their respective roles in Internet governance is crucial.

The IGF platform provides a safe space for stakeholders to convene and discuss issues related to WSIS. In this regard, speakers were supportive of the IGF receiving a permanent mandate as an outcome of the WSIS+20 review. The IGF should continue to preserve its multistakeholder nature and approach. Specifically, the APrIGF is an important platform for Asia Pacific voices to be heard in the review process.

There is a need to improve coordination of stakeholder organisations across the Internet governance and digital governance ecosystem. For instance, in their consultation efforts, governments have sought to understand the complexities, challenges, and gaps that persist.

Further, through iterative feedback from multistakeholder networks, they are able to test ideas and refine positions in preparation for the United Nations General Assembly (UNGA).

Speakers emphasised that capacity building was also required to enable full participation particularly for under-represented economies and stakeholders. Separately, the WSIS+20 outcomes could highlight the role of community-centred connectivity (CCC) in connecting the unconnected around the world. This particularly in the APAC region which is diverse with Least Developed Countries (LDCs), Landlocked Developing Countries (LLDCs), and Small Island Developing States (SIDS).

As the WSIS+20 Review is a pivotal moment for the global Internet governance ecosystem, it is essential to strengthen regional collaboration in APAC, providing input and contributing towards the process.

Track 1: Access & Inclusion

“Access and Inclusion” is a critical part of digital governance, as any governance discussion must move from rhetoric to reality—transforming access into meaningful participation that benefits all. In the context of the Asia-Pacific (APAC) region, access and inclusion is a broad topic that spans across disability inclusion, gender equality, youth empowerment, digital literacy, artificial intelligence (AI) governance, and community connectivity. In this, ***a clear throughline has emerged:*** digital access is no longer a matter of infrastructure alone, but of justice, equity, and agency. Inclusion of youth voices are also necessary to ensure inclusion is ingrained in every part of society. It is about a vision of inclusion grounded in local context yet ***united by a shared principle:*** that the digital future of the region must be built with its most marginalised voices, not merely for them.

During the APrIGF 2025, experts from governments, civil society, academia, and the private sector called for a human-centric and rights-based approach to digital access, inclusion and transformation—one that embeds accessibility, diversity, and accountability at every layer of Internet governance. In a significant way, it hosted and discussed key Access and Inclusion themes and areas - Access and Persons with Disabilities; Gender and Inclusion; Youth and Access; Digital Literacy and Universal Accessibility; Role of AI in Access, Inclusion and as a Public Good.

Digital Inclusion for All

Access, Inclusion & Persons with Disabilities

There is an urgent need to advance inclusive digital governance for Persons with Disabilities (PWDs) in the APAC region, emphasising that innovation often outpaces inclusion. The core principle advocated is that Persons with Disabilities must be full participants and co-designers of policy and infrastructure, not merely subjects of support or consultation. Digital governance must be viewed as an issue of power, participation, and justice, where accessibility is a right and a democratic necessity. Achieving this requires representation (Persons with Disabilities at the decision-making table), policy enforcement (allocating resources and enforcing accessibility standards), and collaboration among policymakers, technologists, and organisations of persons with disabilities or Disabled People Organisations (DPOs). Despite growing awareness and

policy references to disability inclusion, enforcement, coordination, and meaningful participation of Persons with Disabilities remain inconsistent across the region. ***"Nothing about us without us"*** must move from slogan to statute. True inclusion of Persons with Disabilities means dismantling tokenism. DPOs must not be excluded in any policy development process[3].

There are 3 key systemic "A" challenges as barriers faced by the Persons with Disabilities community: (i) Adaptability (the negative mindset that Persons with Disabilities cannot use technology); (ii) Affordability (Persons with Disabilities are often considered liabilities, limiting family investment in accessible devices); and (iii) Accessibility.

The major accessibility barrier is that technology is developed without meeting accessibility standards. Examples include government documents not adhering to Unicode standards and the lack of alternative text for graphics on websites, rendering them inaccessible to screen reader users. Nepal, for instance, has a critical need to ratify the Marrakesh Treaty, an international human rights instrument that provides a copyright exception to the blind and print disabled, enabling the production of teaching and learning materials in accessible formats like braille or digital content. In Indonesia, many policies still fall short, lacking clear statements or standards for digital accessibility and focusing primarily on physical infrastructure, and a national-level guideline under the Ministry of Digital Communication remains unsigned. Furthermore, a significant talent gap exists, as accessibility is rarely taught in universities, and awareness of the Web Content Accessibility Guidelines (WCAG) accessibility standard is nearly non-existent among platform developers and policymakers.

Solutions must involve embedding inclusion from the start. Since AI is a data-driven technology, if Persons with Disabilities are not included from the beginning—in designing, data collection, and interface—the resulting model becomes biased and may fail to recognize diverse inputs, such as speech impairments. Therefore, inclusion must be embedded from the first line of code to the prototype.

All designers must apply the WCAG before finalising their products, which can be tested using the World Wide Web Consortium (W3C) test. Technologists also advocate for community-owned platforms and decentralised technology, such as locally accessible WiFi networks and the Stories. As an example, Janastu.org platform in India allows people to record their stories and

[3] APrIGF 2025, "Nothing About Us Without Us: Advancing Inclusive Digital Governance for Persons with Disabilities in Asia-Pacific". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2NjM1ZWFjNWMxYy8vMzkvLzIzNjIvLzA= (last accessed 8 December 2025)

narrate content without needing to read or write. This approach expands the definition of "disability" to include people who cannot read and write (nearly half of India), a large, marginalised group that most Western guidelines fail to consider.

The way forward requires political will and systemic governance reform, not just isolated projects. The importance of political will, cross-sector collaboration, and early inclusion of accessibility principles in research, education, and emerging technologies such as AI and Internet of Things (IoT) are the must priorities. Governments must invest adequate funds and introduce affirmative action for technology development, devices, and accessible content preparation for Persons with Disabilities. Sustainable funding and partnerships can ensure disability-inclusive practices become long-term standards, not short-term projects.

Specific calls are made for the e-Governance Commission of Nepal to ensure the participation of Persons with Disabilities and women with disabilities, who face additional barriers due to inaccessible e-governance platforms and limited representation. Key suggestions included: strengthening policy enforcement by adopting measurable accessibility standards, conducting regular audits of public digital platforms, and allocating dedicated budgets; and institutionalizing representation by giving Persons with Disabilities and DPOs permanent seats within digital policy committees and national Information and Communication Technologies (ICT) councils.

As the digital transition advances, accessibility and equal access continue to be problematic. There is a need for incorporating next-generation guidelines to ensure digital accessibility for Persons with Disabilities, aligned with the principles of universal design, interaction experience (IX), and secure design practices. Digital literacy programs tailored for Persons with Disabilities (especially women, rural, and low-literate users), local language accessibility, affordable assistive technologies, and open-source innovations are needed to ensure that meaningful participation of Persons with Disabilities is fundamental to achieving equitable digital governance. The issues around identification of inaccessible platforms and tokenistic consultations are seen as no lesser truth.

Inclusion of Persons with Disabilities also means that individual representation of Persons with Disabilities should be associated with participation and ownership of DPOs in forums and platforms. The real digital governance which is not token should involve people with disabilities and not as subjects who are to benefit from such initiatives but also as agents of change and decision making in policy processes that are inclusive.

Digital governance in the APAC region can become genuinely inclusive by embedding accessibility, participation, and representation of persons with disabilities at every level of policymaking and system design. Policies must ensure Persons with Disabilities, especially youth, women, and those in rural areas, have equal access and influence in digital decision-making. Mainstreaming Persons with Disabilities' participation in governance agendas should be a shared responsibility of all sectors.

Gender and Digital Inclusion

Gender inclusion related to digital matters in Asia Pacific should move beyond rhetorical commitments to tangible and measurable action. The core theme is shifting the conversation from socio-cultural perspectives to the significant socio-economic impact of the digital gender divide.

A research on "connected resilience" illustrated that mere Internet access is insufficient without meaningful connectivity—consistent, affordable, safe, and empowering use of digital technologies[4]. The study found that women are significantly left behind in meaningful connectivity, and this exclusion has a massive financial cost: Middle-Income Countries were calculated to be losing nearly half a billion U.S. dollars in their economies in 2023 due to women operating outside the digital economy, or may cost half a trillion dollars in the next five years. Closing this gap requires a multi-stakeholder approach, deep investments, and focus on women specifically.

Onica Makwakwa's framework for action is the RIYAL framework (though the full acronym is presented as R-E-A-A-L-C-T), which emphasises: Rights (Human Rights-based approach), Education (for digital transformation), Accessibility and Affordability (including devices), Language and Content (relevant content in local language), and Targets (setting realistic, time-bound goals).

National frameworks and implementation efforts are vital, but face significant governance challenges. As an example, Pakistan's pioneering Digital Gender Inclusion Strategy launched through the Pakistan Telecommunication Authority (PTA) in 2024 demonstrates national-level interest, built on extensive research into barriers. The Strategy established five Working Groups to address: access/affordability, data scarcity, digital skills, societal perception that women don't

[4]APrIGF 2025, "Prioritising Digital Gender Inclusion in Asia: From Token Mentions to Transformative Action". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2NmIzYWY0MjAyNy8vMzkvLzIzNzQvLzA= (last accessed 8 December 2025)

need the Internet, and safety/security. However, implementation faced challenges including overlapping mandates between ministries, lack of reliable data, and the difficulty of getting various government organisations to prioritise the gender agenda over their own established goals. These issues reflect a broader regional need for clearer coordination mechanisms.

A critical gap remains in gender-disaggregated and disability-inclusive data. One may know the speed of a network in a rural area, but don't know how many women/marginalised groups can afford a data plan or own a smartphone. Many gender identities are still underrepresented in surveys. This is a very valid and important concern — gender- and disability-disaggregated data are indeed essential for building a more inclusive digital landscape. However, the current focus is slightly different, which may be looking at the discrepancies between project-reported data and the actual experiences of users, irrespective of their gender or economic background.

Civil society stresses the necessity of co-designing solutions with, not just for, women and gender-diverse individuals. The Asia Pacific Network Information Centre (APNIC) Foundation's *SWITCH Program* is seen as an example, empowering over 600 women and gender-diverse individuals to develop digital and leadership skills, as well as to build and sustain Internet and digital infrastructure, across 6 economies across Southeast Asia, supporting a cohort of about 150 participants annually. A call is required for "collectivising impact"—pooling resources across sectors to avoid duplication and scale up successful interventions.

Online safety is a critical barrier disproportionately faced by women. Private sector accountability is critical. As an example, Meta highlighted its commitment through clear policies, proactive engagement, and technological safeguards. The specific tool StopNCII.org is highlighted as an industry initiative built and funded by Meta in conjunction with the Revenge Porn Hotline. This tool prevents the sharing of nonconsensual intimate imagery (NCII) by generating a unique hash of the image that is shared across Meta's systems and industry partners (e.g., Crown, Bumble) to prevent its upload, without storing the original image.

Effective risk mitigation requires sustained collaboration between tech companies, civil society, and regulators. Furthermore, gender digital inclusion extends beyond access—it must encompass agency, skills, and representation. Inclusion strategies must adopt intersectional approaches that serve Persons with Disabilities and gender-diverse communities, noting that the absence of gender-disaggregated and intersectional data remains a major obstacle to informed policymaking.

Digital gender inclusion must evolve from aspiration to a shared responsibility and a collective societal commitment. Future strategies should integrate access with education, motivation, and cultural change to foster meaningful engagement. The call to action is to transform equality commitments into measurable, long-term practices and to institutionalize inclusive design within digital governance, ensuring women and marginalised groups are not just connected, but truly empowered to shape their digital futures.

Youth & Access

True digital governance begins when every young voice, especially the unheard, shapes the future with equal power and purpose. For youths, there exists structural barriers to digital access, policy literacy, and participatory mechanisms that continue to marginalise them, particularly those from rural, displaced, or underserved communities.

Despite youth in the APAC region being among the most connected globally, they remain structurally excluded from Internet governance[5]. In the Pacific, inclusion starts with affordability and devices and priorities starts with wholesale price transparency, social tariffs for students and low-income households, community Wi-Fi at schools and libraries, and micro-financing for entry-level smartphones with built-in accessibility features.

This exclusion is compounded by a significant skills gap; the 2025 United Nations Educational, Scientific, and Cultural Organisation (UNESCO) report highlights that 450 million young people lack adequate skills for a modern job market, threatening to leave a generation behind as AI reshapes the economy. Additionally, nearly 40% of teachers in Southeast Asia report insufficient training in digital technologies, directly impacting students' digital literacy.

The challenges are deeply entrenched in the APAC context. Over 60% of the APAC region lacks Internet access. One of the reports suggested that in Indonesia, up to 24,000 villages still lack Internet access, with one province alone having a digital "blind spot" affecting 196 villages and approximately 30% of the area. Research data in this area is still underdeveloped, however, these early reports reflected that in such rural areas, education is poor, and many young people lack future plans because they are cut off from the global market. Similar issues regarding a lack of technology, energy, and Internet in rural areas are also faced in Sri Lanka. These structural barriers mean that meaningful connectivity, digital literacy, safety, and governance participation

[5] APrIGF 2025, “Bridging the Digital Divide: Youth Access to Knowledge, Policy, and Power”. Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2Q0MGFkZWVhNC8vMzkvLzI0MTcvLzA= (last accessed 8 December 2025)

must be recognized as indicators of well-being. To highlight, young women and LGBTQ+ youth in some economies may face compounded digital exclusion due to stigma, infrastructure gaps, and lack of targeted literacy programs.

Recommendations concerning the affordability challenge for youths includes exploring government subsidies and leveraging Corporate Social Responsibility (CSR) to improve access. Critically, any plan must be founded on net neutrality, ensuring that subsidised access does not mean lesser quality content compared to what those who pay more receive. Regarding the design challenge, which addressed policy illiteracy, exclusion, and linguistic diversity (e.g., Indonesia's 700+ dialects), recommendations included fostering harmonised approaches and "one voice" from communities of interest before broader publicity discussions.

It is advised that technical forms must be sorted out to ensure universal design and accessibility, avoiding reliance on a single language. Addressing the tokenism challenge, which tackles youth participation being limited to elites with institutional credentials, recommendations seeks to make participation structural, not symbolic: this included guaranteed spots for youth from rural, underserved, or marginalised communities at summits, and implementing pre-summit education and community dialogues/online consultations in local regions, valuing lived experiences over credentials.

The core message is that youth must be recognized as essential co-governors of the Internet's future, not merely as beneficiaries or a separate, token stakeholder group. Currently, young people are often included symbolically, treated as a "checkbox" in consultation processes. Instead, their digital fluency, global outlook, and innovative capacity should be fully embedded across all existing stakeholder groups including government, civil society, and the private sector, to ensure true intergenerational collaboration.

To make their participation meaningful, youth should be treated as a precisely defined social group, like "Legal Experts," and given formal, accountable positions with specific responsibilities, mentorship, and opportunities for professional development. The principle of "Nothing about us without us" demands that youth hold formal co-decision-making roles from the pre-policy stage, such as formalized voting seats and ring-fenced budgets for youth-led projects.

The APAC youth emphasises three key priorities: (i) explicitly recognizing youth as co-creators in Internet governance; (ii) committing to closing the digital divide by addressing gender,

linguistic, and cultural equity alongside connectivity; and (iii) ensuring responsible innovation by engaging youth in capacity building and developing ethical and sustainable frameworks for emerging technologies. Ultimately, their voices must be heard and actively embedded into decision-making to build an inclusive future.

A call to action, captured in a call to draft a youth access manifesto, advocates for inclusion, empowerment, youth participation, and localised outreach. There is agreement on the necessity to move beyond tokenistic youth inclusion toward co-creation and agency in shaping the digital future. The priorities include: integrating digital equity and well-being frameworks; institutionalizing youth participation in digital governance design and evaluation; promoting intersectional and localised data to inform inclusive policy; and recognizing digital exclusion as a structural barrier to opportunity and dignity. That meaningful youth inclusion requires not just access to technology, but access to decision-making spaces, capacity-building, and sustained mentorship. Digital access alone is not enough; meaningful youth participation requires access, policy literacy, and structural inclusion. Youth inclusion must move beyond tokenism, being offered spaces where young people can actively shape outcomes, not just attend consultations.

Emerging technologies must advance ethically, inclusively, and sustainably. The call is for youth engagement in capacity building, research, and advocacy, as well as frameworks to measure and minimise the environmental impact of digital infrastructure. Stakeholders call for stronger commitments to linguistic accessibility, rural and remote access, and targeted digital literacy initiatives enabling APAC youth to fully benefit from digital participation.

Psychological studies of youth and their digital lifestyles, as well as exploring the impact of gender diversity on promoting secure internet governance is called for. Furthermore, incorporating AI, Quantum AI, or Artificial General Intelligence (AGI)-based policy frameworks and digital risk management systems by governments or other relevant stakeholders could support sustainable and secure digital services. There is a need for fostering an intergenerational co-leadership model to ensure youth is involved in important parts of governing the Internet.

The ideal outcome is for youths to be integrated in all groups of stakeholder, while having a standalone youth group to secure its presence and function as digital ecosystem co-creator.

Digital Literacy and Accessibility for All Ages and Abilities

One critical issue of the digital divide is, being connected is not the same as being included. Beyond simple Internet access there is a need to address gaps in digital literacy, accessible technology, and meaningful inclusion for various groups, including Persons with Disabilities, senior citizens, and linguistic minorities[6].

Specific systemic challenges face different groups. For visually impaired persons, the foremost barrier is inadequate labeling or lack of information for screen readers. A simple example is an unlabeled button on a webpage, which renders the entire process inaccessible because the screen reader only pronounces "button," and the user can't determine its function like submit or cancel. In terms of Linguistic Inclusion, many local languages, such as Nepal's 120+ languages, lack updated assets and full access to large language models (LLMs) which are primarily developed for highly resourced languages. For Senior Citizens, they face a transitional problem as they lack a background in the new technology and may develop multiple failing faculties. This makes them vulnerable to payment scams like those involving Quick Response (QR) code fraud, even though technology use (like Unified Payment Interface or UPI) has become widespread. The digital transformation must not overlook those who face systemic barriers, such as complex interfaces for older adults, inaccessible design for Persons with Disabilities, and unsafe online environments for gender minorities.

There is a need for a more explicit focus on engaging underrepresented communities, particularly in rural and remote areas of the Asia-Pacific region, and understanding their digital cultures, needs, and barriers. Digital inclusion must address not only connectivity, but also gender, linguistic, cultural, and geographic equity.

There is a need for more detailed digital education programs tailored to diverse cultural and linguistic contexts within the region, as well as addressing technological challenges and solutions provided by service providers and International Telecommunication Union (ITU). A key focus is linguistic inclusion, highlighting the need for local content creation and the development of technologies that support low-resource languages, thereby making the Internet more relevant to the region's rich linguistic diversity. This includes supporting multilingual internet access

[6] APrIGF 2025, "Beyond Connection: Fostering Digital Literacy and Accessibility for All Ages and Abilities". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2ODE5MjVjZjlhZS8vMzkvLzI0NDgvLzA= (last accessed 8 December 2025)

through Internationalised Domain Name (IDN) adoption and Email Address Internationalisation (EAI).

Policy and private sector intervention are crucial to achieving "accessibility by default". Private companies are primarily motivated by the business case, as developing accessible products allows them to reach a wider audience, including Persons with Disabilities and those with age-related disabilities. However, proactiveness comes from a push via national or global policy. Regulations at the state level (like in the US or European Union) compel compliance, which is why major tech companies like Apple (iOS) and Microsoft (Windows) include screen readers and magnifiers.

The European Accessibility Act, which came into force in June 2025, mandates that any digital service supplied in the European Union (EU) must be accessible to EU citizens. This will impact Asia-Pacific companies that outsource digital services to the EU, threatening their bottom line if they are not compliant. It is easier to build a product accessible from the start than to retrofit accessibility later. Furthermore, features initially developed for Persons with Disabilities, such as captioning, are now widely used by non-disabled people for numerous purposes.

The state of digital accessibility in the Asia-Pacific region has a long way to go. Governments and civil society must collaborate to embed standards like the WCAG into policy frameworks. Academia also plays a vital role: university curricula should integrate web accessibility and AI/digital literacy courses. Academic institutions can serve as technological innovation hubs by leading language documentation and translation projects, and by developing local LLMs tailored to the characteristics and needs of local languages. As an example, Nepal's federal structure has increased the demand for local language tools in government platforms.

Inclusion, trust and accountability are not accidental. They must be built. Our digital future depends on intentional design – of systems, of governance, and of spaces where people can connect, listen, and build together. Ultimately, success is contingent on collaboration across sectors including government, private industry, academia, and civil society to promote a digitally equitable APAC region. The Internet is for everyone, and that’s why the future of digital cooperation is at stake. It depends on all of us to connect, listen, and build together.

AI for Justice & Public Good

There exists a complex relationship between private investment, public infrastructure, and public accountability as governments across APAC conceptualise and deploy AI for welfare objectives in sectors like banking, healthcare, and education.

National strategies and policies in countries including India, Singapore, Malaysia, and Indonesia reveal that attracting large-scale private investment to expand technological capabilities and rebranding government efficiencies are two key motivations for states[7]. This reliance on private capital, often facilitated through Public-Private Partnership (PPP) models, for scaling AI raises significant governance questions on the necessary safeguards. The financial commitment to AI varies across the region: India has pledged $1.12 billion towards building its AI ecosystem, focusing on data centers and educational courses. The Philippines is earmarking initial investments primarily for health care, education, mobility, and environment sectors. In contrast, Nepal currently operates with no specific budget for AI, with its advancements driven predominantly by the private sector, although a national AI center is engaging with private partners. A key structural challenge across these nations is the lack of transparency in budgeting and performance evaluation, which hinders the ability to track the actual public value added by these AI initiatives.

The deployment of AI, particularly in sectors like smart city infrastructure, urban management, and healthcare, introduces critical concerns regarding data ownership and governance. An example from an Indian smart city illustrates privacy risks where sanitation workers must wear Radio Frequency Identification (RFID) tags that track movement and record conversations and photos, with the collected data being owned by a third-party private organisation. A severe accountability failure in the Philippines saw a private entity collect citizens' data via a QR code system during the pandemic without government approval and subsequently sell the data to marketing agencies. Furthermore, historical social and spatial biases (e.g., gender, class, caste) are often replicated and amplified in AI systems due to inherent bias in datasets. Examples include AI-based risk assessment in the financial system failing to meet the objective of financial inclusion because of historical disparities reflected in the data. The inclusion of AI in systems like automated security checkpoints using facial recognition or QR codes (like those seen in

[7] APrIGF 2025, "AI as Public Good: Analysing the interplay of Private Investments, Public Infrastructure and Public Accountability". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2ODE1MzkxYWUxYS8vMzkvLzI0NDYvLzA= (last accessed 8 December 2025)

Singapore or Indian airports) is critically seen to expand and reshape surveillance over citizens' bodies and mobility.

The quality of data and the legitimacy of its sources have always been among the most contentious issues in AI governance. This situation closely resembles the copyright debates that emerged during the early days of the Internet, when online creators fiercely contested how their works were copied and reused. In today's AI era, however, the focus of contention has shifted. For governments to ensure that AI applications are trustworthy and accountable, the data lifecycle must be treated as a central pillar of governance, not merely a technical process.

True inclusion means not just having access to the Internet, but being represented in the languages and data that shape the digital world, especially as AI becomes more embedded in our lives. AI systems learn from the data we feed it, so if most online content is in a few dominant languages, then the technology ends up understanding only part of the world.

In the justice sector, AI can be seen fundamentally as an assistant to the judge, not a replacement for human wisdom[8]. While AI can enhance efficiency and access, like through India's eCourt project or a company in Nepal using AI to translate complex legal documents into simple Nepali, the consensus is that the "sacred line" that AI must never cross is the final judgment, empathy, and nuance, which must always remain with a human judge. Potential areas for AI use in justice identified by the Supreme Court of Nepal include case management, legal research, evidence analysis, and judgment assistance. For accountability, a shared accountability model can be proposed, where developers ensure industry standards are met, and end-users are accountable, although judicial officers bear the major accountability for the outcome, as they must apply their human mind and caution when relying on AI-produced data.

The paramount challenge remains the massive digital divide, which makes relying on digital technology for access to justice a "far away dream" in countries like India. The consensus is that digital inclusion must precede automation to avoid "automating exclusion". True integration of AI goes beyond mere installation, requiring digital literacy and equitable access for all. To ensure public trust, ethical governance is essential, requiring adherence to principles like human oversight, accountability, bias mitigation, inclusivity, accessibility, and contextual adaptation, as outlined by the UNESCO's AI guidelines. All emerging technology, including AI, depend on

[8] APrIGF 2025, "AI4Justice: Bridging the Access Gap or Deepening the Digital Divide in the Asia-Pacific?". Proposal form and session report accessible at: https://forms.for.asia/proposal/?proposalform=Njg2NjhkOTI1Y2Y1OS8vMzkvLzIzNzEvLzA= (last accessed 8 December 2025)

robust and resilient Internet infrastructure. The focus on AI and building AI capabilities must not take us away from continued investments in Internet and digital infrastructure and capabilities. The way forward requires strengthening digital foundations through infrastructure, education, and legal reforms , with a call for state-led efforts in funding and reform since access to justice is a fundamental right.

AI should be functional, not mythical. While the concerns raised about algorithmic bias, opacity, privacy, and digital divide are legitimate, they tend to overstate the inherent power of AI itself. AI should not be treated as an omnipotent “black box” that autonomously creates risks; rather, it should be understood as a set of functional tools, each defined by its purpose, dataset, and scope. AI systems learn from the data we feed it, so if most online content is in a few dominant languages, then the technology ends up understanding only part of the world.

To address these issues effectively, the focus must shift from AI’s output to its inputs. The training datasets, not only the algorithms, are the real determinants of fairness and accountability. Instead of building massive, all-purpose systems, we should promote smaller, function-specific AI models trained on domain-relevant, well-curated datasets. This modular approach enhances transparency, reduces systemic bias, and allows for more targeted oversight.

Disconnect between Projected Internet Coverage and Real User Experiences

Projects like the "Garden of Connectivity" have been initiated to address a critical discrepancy between official Internet coverage figures and actual user experiences in the APAC region, particularly in India, Malaysia, and Indonesia[9]. The project was motivated by skepticism toward government-promoted figures, such as Malaysia’s claim of 96% 4G coverage in 2021, noting that coverage statistics often fail to capture real-world Quality of Service (QoS) issues. The Project identified three major issues: (i) performance monitoring often relies on key performance indicators (KPIs) like download speed, packet loss, and latency, which are not user-centric; (ii) existing internet coverage maps are mainly designed for other stakeholders and are not user-centric; and (iii) policymakers themselves often lack detailed, actionable connectivity data

[9] APrIGF 2025, “A Garden of Connectivity: Visualizing the Internet Connectivity Landscape”. Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2QwNDFkNzhjYS8vMzkvLzI0MTIvLzA= (last accessed 8 December 2025)

for their locality. Nevertheless, the importance of shifting from coverage-centric to quality-centric metrics in connectivity evaluation cannot be overlooked.

To address these challenges, the Project research team introduced several innovations: (i) the myspeed.site open-source platform for user speed tests; (ii) an interactive visualisation component for policymakers; and (iii) the NetStethoscope, an IoT device for ongoing, 24-hour coverage monitoring and localised data collection. The key innovation, the "Garden of Connectivity" visualisation, uses a flower metaphor to present complex QoS data intuitively, making it readable for a "common man" and people with low digital literacy.

In this metaphor, (i) lower petals reflect QoS parameters, (ii) upper petals show telecom provider performance, (iii) a leaf indicates full QoS compliance with regulatory standards (e.g., General Quality of Service - GQS), and (iv) the bark colour distinguishes urban from rural areas, highlighting the digital divide. The bloom's color corresponds to a specific telecom provider, enabling intuitive brand recognition.

Field experiments in Malaysia and India revealed surprising and unpredictable connectivity patterns. In Malaysia, testing in Sarawak showed that while urban areas generally performed slightly better, connectivity quality was often disbursed and unpredictable. For example, the remote area of Long Lamai, accessible only by twin otter flight or four-wheeled drive (4WD), demonstrated stronger network performance than nearby urban centers, while neighboring Long Banga showed poor results. In India, where internet download speeds have increased by 300% over the last 10 years and rural density increased from 43.96% to 59.16%, testing was conducted in a rural area near Hyderabad across four service providers (Jio, Airtel, Vodafone, and BSNL). The visualisation results showed that in the tested rural area, Airtel was performing well, meeting QoS requirements (download, upload, latency, and packet loss), while in the urban area (Hyderabad), Jio was meeting the QoS standards. These findings underscore the need for localised diagnostics and empowering communities with self-assessment tools to advocate more effectively for improved connectivity.

From such projects, the way forward emphasises strengthening community engagement by empowering local populations, particularly in underserved and indigenous areas, to carry out their own connectivity assessments using tools such as myspeed.site. It is crucial to enhance localised data collection by expanding the deployment of NetStethoscope devices and encouraging frequent data collection. On the policy front, there is a need to encourage

policymakers to prioritise quality-based metrics over mere coverage statistics and leverage user-generated data to guide infrastructure investments and regulatory choices. Regional collaboration must also be strengthened to promote the sharing of knowledge and approaches across countries in the Asia Pacific to replicate successful initiatives and amplify their impact.

Track 2: Innovation & Emerging Technologies

Inclusivity in Digital Policymaking, Particularly on Youths' Role

Digital transformation should be inclusive, equitable, rights-based, and people-centred. Digital governance policies should embed these factors by design, and not be treated as an afterthought, to ensure a sustainable digital future[10]. Digital policymaking should consider actionable and sustainable policies, ongoing engagement with multistakeholders, and continuing conversations with marginalised groups who may be excluded from the process.

Focusing on Nepal as an example, key barriers faced to achieve the above include local policies and governance structure, geographical and access challenges, digital literacy gaps, and a lack of meaningful connectivity. Local fiscal and tax policies adversely impact the affordability of services, and Nepal's transition to a federal structure has caused institutional governance hurdles, slowing service delivery at the local level. Geographical challenges for infrastructure in rural areas lead to uneven service delivery between urban and rural areas. Expanding connectivity often only focuses on coverage (quantitatively) but not actual meaningful connectivity ensuring citizens are able to afford the services and devices as well as building digital literacy skills.

To strengthen the inclusivity and accountability of digital transformation, outcome-based testable safeguards should be introduced for Digital Public Infrastructure (DPI) and Artificial Intelligence (AI) systems. This includes pre-deployment risk assessments, red-teaming protocols, incident disclosure standards, and post-deployment monitoring tailored to the Asia Pacific (APAC) context, particularly addressing multilingual disinformation, gender, caste, and class-based harms, and low-resource misuse scenarios.

DPI programs should also adopt a binding rights-by-design checklist, ensuring data minimisation, proportional authentication, verifiable consent, and grievance redress mechanisms with independent oversight. Procurement contracts should embed auditability, exit clauses, and meaningful stakeholder participation from design to decommissioning which is not limited to token consultations.

[10] APrIGF 2025, "Inclusive Digital Policies in Asia-Pacific". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2ODQyYjc4OWNmOC8vMzkvLzI0NjkvLzA= (last accessed 8 December 2025)

To reduce dependency on closed markets and models, the APAC region could pilot a "public-interest compute and evaluations facility", pooling shared compute resources, multilingual benchmarks, and open datasets for low-resource languages. Such regional collaboration would directly support evidence-based policymaking, open science, and culturally grounded safety standards.

Global principles such as the United Nations Development Program (UNDP) Principles and United Nations Educational, Scientific, and Cultural Organisation (UNESCO) Rights, Openness, Accessibility, and Multistakeholder participation for Cross-cutting Issues (ROAM-X) must be locally adapted and operationalized. The UNDP champions "design with the user", which involves using service design blueprints to map actual citizen experience and identify points of exclusion. The UNESCO ROAM-X framework shows that policy translation requires strong political commitment and the institutionalization of multistakeholder advisory boards for effective follow up and implementation. Success requires coordination across all stakeholders, including governments, private sector, civil society, and others.

Youth is also a key stakeholder in the policymaking process as policies defined today will be inherited tomorrow by youths. Concurring with the concept of "design by/with the user", youths should act as co-governers and represent equal voices as any other stakeholders and experienced participants in Internet governance discussions and policymaking[11]. Digital inclusion is not just about access and connectivity, but also representation and shared/equal "power". This also includes addressing linguistic, digital, and so-economic barriers that may limit participation from marginalised youth communities.

Youth engagement must be institutionalized, perhaps through a formal mandate (such as advisory councils, co-lead positions), to legitimize their roles in the regional and global Internet governance ecosystem. Inter-generational collaboration and mentorship, paired with peer support, are key to ensure participation from all "generations" and continuity in knowledge transfer. The APrIGF model is a good example, where experienced community members are paired with younger co-coordinators as a practical way to create a "learn-by-doing" model.

[11] APrIGF 2025, "Not Just Participants: Youth as Co-Governors of the Internet". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2ODRjMmZkYzgzYy8vMzkvLzI0NzQvLzA= (last accessed 8 December 2025)

AI Governance

APAC, home to the world's largest youth Internet user base, is witnessing a sharp rise in human-mimicking Artificial Intelligence ('Social AI'), raising urgent concerns especially for young users' wellbeing to ensure safety and accountability. AI governance in the region should move beyond high-level principles toward measurable safeguards, such as regional testing protocols, algorithmic transparency indices, and standardized post-deployment audits.

AI has been a strong topic of interest in the past couple years. While it is important to acknowledge the social and innovation advantages from the development of AI tools and technologies, we also have to pay attention to the potential risks to society and the need for evidence-based, equitable, adaptive, and inclusive policy frameworks. Proactive ethics, simplicity, and positive incentivization/recognition are required for responsible innovation. It may also be worth considering the adverse impacts of AI developments to the original decentralized nature of the Internet – are these tools killing independent websites and Uniform Resource Locators (URLs), and how users used to interact with website information? AI democratizes knowledge through open models and shared data, but it also recentralizes power in the hands of a few who control data and algorithms.

It is essential to balance encouraging innovation through AI and accountability through regulation. Unregulated or poorly regulated ecosystems may deepen exclusion and harm to marginalised communities (e.g. women, youth, rural communities, indigenous groups). Regulations need to consider addressing capacity gaps in developing subregions (e.g. South and Southeast Asia) including targeted digital literacy programs, ensuring affordable access, mitigating algorithm biases, and enhancing multilingual inclusion such as encouraging development of local language AI tools[12].

An example on balancing innovation with regulation could be Japan's soft-law approach to AI governance which emphasises voluntary business compliance rather than hard regulation, offering valuable insight for agile governance. While it supports innovation and reduces rigidity, such frameworks must ensure inclusion of Small, Medium, Enterprises (SMEs) and prevent malicious misuse. In high-risk sectors like healthcare or autonomous driving, Japan's model

[12] APrIGF 2025, Regulating AI Beyond the Hype: Evidence, Equity, and Policy Priorities for the Asia-Pacific.Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2NzZkOWMwOTM1Ny8vMzkvLzIzODQvLzA= (last accessed 8 December 2025)

balances flexibility with public safety, highlighting that contextual legal and cultural norms shape regional AI policy trajectories.

We need to design inclusive AI systems, then automate it. If we do it the other way around, we're automating exclusion. Systems should also be built for people first, code second. AI should amplify human judgment rather than replace it. A "bias-free" AI system requires delicate balancing as what constitutes bias can be subjective. Also, "removing bias" could potentially compromise the accuracy of AI models.

On bridging capacity gaps, building capacity across both AI sectors and existing regulatory bodies is critical. There is also a need to increase user literacy level, specifically on public understanding of how AI systems work and information on algorithm processes utilised. Establishing regional observatories, fellowships, and policy sandboxes could also aid in institutionalising mutual learning.

Most AI systems also disproportionately favor dominant languages, marginalising smaller linguistic groups– this requires APAC AI regulations to be more regionally contextualized with local datasets to accurately reflect social and cultural diversity, and to promote language justice[13]. Also, AI ethics should be translated to local languages to ensure broader understanding and application. An aspect for consideration could also be to include non-western moral philosophies (e.g. Ubuntu, Sintoism, Confucianism) to address the western-centric approach in AI ethics discussions.

Public–private partnerships (PPPs) are vital to promote equitable AI access and development. Governments must incentivize AI for rural innovation and adopt multilingual AI models to resist digital colonialism. This ensures APAC's local languages and knowledge systems are empowered rather than erased.

Human right principles should also be considered to ensure a human rights-based approach to protect especially vulnerable populations. Taking a rights-by-design approach will ensure human rights and accountability are operationalized through practical, measurable tools, rather than abstract commitments. Policies are also not a "one-size-fits-all". A key element is to involve

[13] APrIGF 2025, "From Oversight to Overlooked: Ethics in AI Governance". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2NmZlZDlhNjBiOS8vMzkvLzIzNzUvLzA= (last accessed 8 December 2025)

grassroots communities and local civil society in AI governance conversations to ensure marginalised communities are not left behind.

In the “Feeling Automated Project” by the Pranava Institute, research was conducted on the current state of social AI systems and its associated risks and harms[14]. The results uncovered worrying behaviours such as disclosure of personal information, self-harm, conversations with AI systems around sensitive topics and to receive advice for children, and others. Other issues would include general safety for minors, erosion of the ability to socialize, self-diagnosis of mental health issues leading to worsened conditions, culturally insensitive outputs, and privacy concerns.

These issues may be exacerbated among the young population, which is predominant in the APAC region. Social AI technologies, which simulate empathy and emotion, must not be allowed to exploit the psychological and developmental vulnerabilities of our young population. While users need to critically assess what we create and consume, technology developers, regulators, educators, and policy-makers are key to ensuring that emerging technologies, like Social AI, do not harm but instead nurture the wellbeing of our future generations.

Stakeholders including policymakers, educators, mental health professionals, and families, need to recognize these risks such as addiction, dependency, and other forms of psychological harms. Potential ways to address such risks are enforcement and audit frameworks, built-in usage limits, re-direction to helpline for users expressing thoughts of self-harm, age verification and safeguards where minors enter into emotional interactions, and others.

Multistakeholder collaboration across governments, civil society, academia, and industry, is required for a comprehensive policymaking process. Public procurement and open-source tool information should be considered towards developing an interoperable and equitable AI governance system.

In the region, several AI policies/frameworks are already in place, including Nepal’s AI policy, Indonesia’s AI roadmap, Philippines’ AI Regulation Act, India’s collaborative AI procurement

[14] APrIGF 2025, “Social AI, Youth and Digital Vulnerability: A call for multi-stakeholder action in the APAC”. Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2UyNDNhN2RjZi8vMzkvLzI0MjYvLzA= (last accessed 8 December 2025)

initiatives. Also referring to a European example, well-curated AI algorithms would filter misinformation and focus on providing results with strong public interest value.

As a region, it is critical to tap on synergies with sharing of data, best practices, and research amongst each other. An example would be Singapore's leadership in AI testing framework and its convening potential for interoperable regional standards through Association of Southeast Asian Nations (ASEAN).

Emerging Technologies and Tools

A Solution to Data Cleaning and Validation for Non-Technical Users– Open Data Editor (ODE)

Open Data Editor (ODE) is an open-source desktop application developed by the Open Knowledge Foundation, aiming to be a non-technical and user-friendly data cleaning and validation tool. The tool prioritizes inclusivity, transparency, and privacy, and addresses the challenge of time consuming data management through detecting, validating, and correcting dataset errors without requiring coding expertise or stable Internet connection[15].

ODE is looking into potential further integration of AI and Natural Language Processing (NLP) technologies to further simplify data correction tasks. Current design choice has focused on use of local AI models rather than large cloud-based Application Programming Interface (APIs), ensuring that user data remains private and secure within their devices (i.e. data sovereignty) and aligning with the rights-by-design approach.

It is important for ongoing capacity building efforts and cross-sector collaboration to make open data tools more inclusive, privacy-respecting, and community-driven through the APAC region. ODE would be useful to support civil society groups in low-resource settings. For instance, integrating ODE with LinkedIn could allow sharing of accurate data and enhancing transparency in professional networks. The aim for ODE is to empower non tech savvy people to use data, and complementary courses by Open Knowledge are also offered to further aid learning of the tool usage.

[15] APrIGF 2025, "Empowering Data for All: Unlocking Trust and Transparency using Open Data Editor". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=NjgzZDc3NWVhMGM3Ny8vMzkvLzIzMzUvLzA= (last accessed 8 December 2025)

A Solution to Sustainable Connectivity at Remote Areas– CurveIQ

Remote telecommunications systems in hard-to-reach areas continue to face serious sustainability hurdles. Many solar-powered sites that bring essential connectivity to these areas break down more often than expected and cost more to maintain. The main reasons include battery wear, poor energy management, and exposure to difficult weather conditions such as high temperatures, humidity, and uneven sunlight.

One of the biggest causes of system failure is premature battery aging. Extreme heat, poor charge management, and long usage cycles shorten battery life, leading to frequent replacements and increased downtime. A large amount of power is also wasted on unnecessary cooling systems and inefficient charging methods, which force operators to invest in larger solar setups and storage units, raising both initial and running costs. Managing such sites from afar requires skilled technicians to keep the battery cells balanced and functioning, adding another layer of complexity, especially for small operators in low-income regions.

CurveIQ aims to overcome these problems through smart and adaptable management tools, combining predictive algorithms and smart control to transform the sustainability of off-grid connectivity It uses weather data to plan charging cycles, manages heat through passive cooling, and balances energy use within the battery bank to prevent uneven wear[16]. The system also includes added features for site safety, backup reliability, and maintenance alerts, helping operators handle remote setups more effectively. This technology could substantially reduce energy waste, improve sustainability, and enhance operational efficiency.

With equipment life extension, energy saving, and operational costs cut down, CurveIQ aims to make remote telecom networks more reliable and affordable. This helps strengthen local expertise, encourages cooperation between regional stakeholders, and supports fair access to sustainable connectivity across the APAC region.

[16] APrIGF 2025, “Powering Sustainable Connectivity: curveIQ's Low-Cost Solution for Remote Telecom Sites”. Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2NzUxNmM0ZTM5Ni8vMzkvLzIzNzgvLzA= (last accessed 8 December 2025)

Track 3: Sustainability

Digital tools can expand access to markets, finance, and new livelihood opportunities; however, the sustainability of this expansion remains uncertain. As India transitions away from coal, efforts to integrate digital technologies into communities such as in Ramgarh and Bokaro regions must address both infrastructure deficits and capacity gaps[17]. Many residents still lack the fundamental digital access and literacy required to benefit from these tools, with women and marginalised groups facing the greatest barriers.

Bridging these gaps requires establishing a two-way perspective: understanding how Internet infrastructure affects the environment, and how environmental challenges, in turn, impact Internet infrastructure. Both dimensions are essential. On the former, investment is needed in green technologies, e-waste recycling, and stronger accountability for technology manufacturers, particularly around reuse, repair, and replacement of parts. Sustainable energy sources must also underpin increasingly intensive digital capabilities.

On the latter, greater investment is required in the cable-repair industry, reinforcing local infrastructure to reduce external dependencies, and developing resilient tools that can support emergency communication even in offline environments. The APNIC Foundation has already supported initiatives to design emergency preparedness and response mechanisms capable of functioning offline, offering valuable models for future resilience efforts.

For a sustainable expansion, reliable and affordable electricity and Internet, digital literacy and skills training, and supporting self-help groups should be developed concurrently to engage in digital markets. Digital solutions may not always be universally beneficial. Emerging sectors such as data centers and gig work must be regulated to prevent environmental harm and to ensure worker protections.

A balanced and inclusive approach to leverage digital technologies where useful, but also grounding the transition in community needs, equitable access, and careful planning are key to ensure sustainability from such technological developments and to avoid deepening existing inequalities.

[17] APrIGF 2025, “Digital Dilemmas in Just Transitions: Lessons from India’s Coal Heartland”.Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2RiMGY3MGQ0NC8vMzkvLzI0MjQvLzA= (last accessed 8 December 2025)

Track 4: Security & Trust

The Internet enables connections across societies, but these connections can also cause significant harm if they are not secure and trustworthy. Unlike typical cybersecurity conferences, the Asia Pacific Regional Internet Governance Forum (APrIGF) approaches this issue through both a technical lens and a human-centric perspective.

The Asia-Pacific (APAC) region, with its diverse mix of developed and developing economies, faces unique challenges while addressing basic development needs, it must also contend with emerging technologies such as Artificial Intelligence (AI) which introduce new dimensions of risks to security and trust.

Strengthening digital security requires examining the fundamental principles that govern Digital Public Infrastructure (DPI). Since DPI deployment often depends on government funding and adherence to local regulations, it is critical to consider how the prevailing Internet governance philosophy like multistakeholderism can be effectively applied to ensure DPI is deployed in a manner that promotes safety and trust.

Ultimately, security and trust must serve the interests of Internet users. The following paragraphs highlight discussions from the APrIGF 2025 on how security and trust can be undermined through various threats, particularly affecting vulnerable groups such as children and individuals with limited digital literacy. It also explores possible mitigation measures, as well as the potential liability and responsibility of online platforms, intermediaries, and AI-powered agents in upholding a secure and trustworthy Internet environment.

Governing Digital Public Infrastructure in the Asia-Pacific

DPI from foundational digital identity document (ID) to payments, registries, and data exchange rails is accelerating across the Asia Pacific. Its promise is real: faster, cheaper, more reliable public services at scale. But DPI is not a neutral construct. Design choices determine whether these systems widen or narrow inequalities, entrench surveillance, and weaken autonomy, or instead strengthen rights, accountability, and trust. In many countries, DPI now mediates access to essential services; that centrality raises the stakes for robust governance that treats people not as data points to be managed but as rights-holders to be protected.

A rights-centric DPI regime starts by acknowledging that today's safeguards are uneven and fragmented. Most governance frameworks privilege individual data protection doctrines while overlooking collective harms such as structural exclusion, cultural erosion, dependency on single vendors, and coercive interoperability that forces people into one ID or platform[18]. Barriers to voice are also systemic. Weak connectivity, inaccessible interfaces, low digital literacy, and constrained civic space disproportionately silence marginalised communities. "Meaningful participation" cannot be a slogan– it must be an operational commitment to include underserved and at-risk groups in agenda-setting, design, testing, deployment, and redress.

To close the gap between policy intent and technical reality, governance must move protections into the stack itself. The IO Foundation's Data-Centric Digital Rights (DCDR) approach is one practical path: treat the "digital twin" as inseparable from the person ("I am my data"); prevent harms by default ("end-remedy"); and encode rights into code ("rights by design")[19]. Operationally, this means purpose-binding every data element, making off-purpose use technically impossible. Building a taxonomy that maps harms→ rights→ controls, so protections are testable; enforcing at the lowest feasible layer (infrastructure/protocols) while surfacing controls in the user interface, and using open technical standards so protections scale faster than law alone. Explainable enforcement —systems that state which right blocked which operation and why – turns abstract safeguards into auditable practice.

Applied to DPI, rights-by-design changes outcomes. In digital ID, it curbs over-collection (e.g., biometrics and life-history), separates logical from physical identity to avoid one-to-one mirroring, and mandates impact assessments, audit trails, minimisation, and automatic expiry. In data exchanges and "smart city" telemetry, it constrains correlational re-identification and secondary use through machine-enforced purpose tags and correlation limits. In cross-border platforms interfacing with DPI, it harmonizes protection via a strictest-common-denominator rights taxonomy across jurisdictions and exposes portability, consent, and redress dashboards to users.

Multistakeholderism must be practiced, not performative. Governance should institutionalize participation of disability organisations, women's groups, youth, indigenous communities, and technologists with decision power instead of post-hoc consultation. Accountability must bind

[18] APrIGF 2025, "Multistakeholderism and meaningful participation in DPI Governance: What should it actually look like?". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2ODAxNDQyZDJkOC8vMzkvLzI0MzgvLzA= (last accessed 8 December 2025)
[19] APrIGF 2025, "Building Rights-Centric Digital Infrastructure: A Collaborative Workshop on the Data-Centric Digital Rights (DCDR) Framework". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2ZlZjQ5MDEyNi8vMzkvLzI0MzYvLzA= (last accessed 8 December 2025)

both public and private actors: clear duties of care, public attestation dashboards, independent audits, incident reporting with time-bound remedies, and procurement clauses that make accessibility, security, and interoperability non-negotiable. Building trust also requires parallel investments in the social layer named digital literacy programs, accessibility by default, local-language interfaces, and open documentation to ensure people can exercise the rights encoded in systems.

A practical outcome of this approach is a policy-engineering checklist for DPI:

(1) **Purpose**: define legitimate, finite purposes per dataset and publish them;

(2) **Proportionality & Minimisation**: collect only what is necessary;

(3) **Encoding of Rights**: implement machine-enforced consent, access, correction, portability, and deletion;

(4) **Accessibility**: apply Web Content Accessibility Guidelines (WCAG) / Authoring Tool Accessibility Guidelines (ATAG) and usability testing with affected groups;

(5) **Security & Resilience**: independent audits, breach response, and verifiable logs;

(6) **Transparency**: open standards, explainable enforcement, public dashboards;

(7) **Accountability**: clear controller/processor duties, sector-specific harm taxonomies, and enforceable remedies;

(8) **Participation**: governance seats and continuous feedback channels for underserved communities;

(9) **Vendor & Lock-in Controls**: interoperability, exit plans, and competition-friendly design;

(10) **Oversight:** independent, adequately resourced bodies with sanction powers.

Governed this way, DPI can be both efficient and egalitarian. The measure of success is not how much data a system acquires, but how effectively it encodes rights, prevents harm, and distributes agency—especially to those who have historically had the least.

The Human Dimension of Security and Trust in the Digital Age

The experience of security and trust online has become an extension of human well-being itself. When personal data moves invisibly across networks, it shapes how people perceive control, safety, and dignity in the digital sphere.

An APrIGF workshop on online privacy and security underscored that the erosion of trust often begins with the smallest acts of disclosure—an innocent quiz, a registration form, or an unexamined app permission[20]. Through such mechanisms, individuals unwittingly reveal personal fragments that, when aggregated, can construct intricate digital profiles capable of predicting and influencing behavior. This process turns the person into a product, reducing human identity to data points, and subtly eroding autonomy.

Online tracking and profiling deepen this sense of exposure. Every click, scroll, and pause becomes a data signal for surveillance capitalism. People are left navigating a digital world where privacy policies are written in inaccessible language, where consent is coerced through dark patterns, and where trust is demanded rather than earned. The psychological toll is tangible—constant awareness of being watched breeds self-censorship, anxiety, and digital fatigue. As personal information becomes currency, vulnerability to hacking, identity theft, and manipulation becomes part of everyday life. This is not merely a technical challenge but a human one: the steady corrosion of the right to exist online without fear.

Security and trust also depend on power relationships between users and platforms. Individuals are continually urged to “protect themselves,” yet the architecture of most platforms is designed to extract, not safeguard, data. This asymmetry of responsibility reinforces helplessness and mistrust. True accountability demands that platforms adopt rights-by-design principles—building security into systems rather than outsourcing it to users. Only through transparent oversight, explainable data practices, and enforceable accountability can the digital ecosystem evolve into one that restores agency and confidence.

Building a trustworthy digital environment therefore requires cultural as well as technical change. Digital literacy must empower people to recognize manipulation, manage their data footprint, and demand ethical design. Yet literacy alone is insufficient without systemic reform as a shared responsibility: regulation, corporate ethics, and cross-sector cooperation must align to

[20] APrIGF 2025, “"Which Animal Are You?" Take a Quiz, Learn More”. Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2U0ZDE2ZGRmOC8vMzkvLzI0MjgvLzA= (last accessed 8 December 2025)

create infrastructures that are secure by default and private by design. Youth-led innovations in online child protection illustrate how empowerment transforms fear into resilience—when users, especially young ones, become co-creators of safety rather than passive consumers of risk[21].

Finally, as AI systems and chatbots mediate more human interactions, security and trust hinge on cultural integrity and inclusivity[22]. Automated moderation trained on Western norms cannot fully interpret the nuance, humor, or emotion of Asia-Pacific societies. When content moderation errors silence voices or misjudge intent, they compromise not just free expression but collective confidence in technology itself. Embedding multilingual, context-aware governance into digital systems is thus essential for human-centric security.

At its core, digital security is not about protecting devices—it is about protecting people's sense of self and belonging in an increasingly datafied world. Trust, once fractured, cannot be repaired by encryption alone; it must be rebuilt through fairness, transparency, empathy, and the recognition that every byte of data represents a human life behind it.

[21] APrIGF 2025, "Smart, Safe, Strong: Youth Innovations for Online Child Protection". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2QyMTY5M2YwZi8vMzkvLzI0MTQvLzA= (last accessed 8 December 2025)
[22] APrIGF 2025, " Local Bots, Global Norms: Discussing content moderation and chatbots in the APAC region". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2M3OWZmMjMyYy8vMzkvLzI0MDkvLzA= (last accessed 8 December 2025)

Track 5: Resilience

The accelerating digital transformation across the Asia-Pacific (APAC) region has pushed questions of resilience to the forefront of Internet governance. As societies become increasingly dependent on digital systems for economic participation, public services, and emergency response, the stability and security of digital infrastructure directly influence national resilience and individual well-being. Yet resilience cannot be understood only as a technical challenge—it is shaped equally by governance frameworks and the financial models that sustain them. The discussions within this document examine resilience across three interconnected dimensions: building robust and inclusive infrastructure capable of withstanding disruption; safeguarding digital ecosystems from regulatory overreach that threatens openness and innovation; and ensuring sustainable, equitable funding mechanisms that empower long-term, community-driven resilience. Together, these perspectives offer a holistic foundation for strengthening the region's digital future.

Infrastructure Resilience

Infrastructure resilience in the Asia-Pacific region must be understood as both a technical and social imperative. As climate-related disasters intensify, the stability of digital systems has become directly linked to human safety, economic continuity, and the protection of fundamental rights. Across multiple regional experiences, digital disruptions—whether caused by undersea cable failures, earthquakes, floods, or deliberate shutdowns—have demonstrated that connectivity now functions as a critical layer of crisis response[23]. Where infrastructure lacks redundancy, entire populations are left without access to early warning systems, emergency coordination mechanisms, or vital information flows.

A resilient digital ecosystem requires diversification of connectivity technologies and the elimination of single points of failure. Traditional reliance on centralized cable-based systems has proven insufficient. The region must adopt hybrid models that integrate fiber, microwave, and satellite connectivity, ensuring that disruptions to any single system do not isolate communities. The introduction of satellite networks in countries such as Bhutan reflects a broader shift toward decentralized architectures that remain operational even when terrestrial

[23] APrIGF 2025, "Disasters, Data, and Digital Rights". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2ZlMjU5MWEyYi8vMzkvLzI0MzQvLzA= (last accessed 8 December 2025)

infrastructure is compromised. Expanding operator diversity is equally important; markets dominated by one or two providers are more vulnerable to catastrophic breakdowns, whereas multi-operator environments naturally embed redundancy.

Infrastructure resilience also hinges on addressing the paradox of digital equity. Communities with the least reliable connectivity—rural, remote, indigenous, or marginalised—face the gravest risks during disasters. Yet commercial deployment models often overlook these groups, widening the digital divide and compounding vulnerability. Examples across the region highlight the consequences: coastal communities in Bangladesh unable to access online forecasts, students in the Philippines losing months of schooling due to poor networks, and populations in Myanmar left intentionally disconnected during periods of instability. Ensuring resilience therefore requires integrating equity into infrastructure planning through subsidised access, universal service obligations, and targeted investment in climate-vulnerable areas.

Human capacity forms a second pillar of resilience. Technology alone cannot safeguard communities without digital literacy, preparedness training, and public awareness of infrastructure locations and emergency communication channels. Countries that have combined physical resilience with human capacity building—such as Japan—demonstrate more effective crisis response and faster recovery. Post-disaster initiatives in Tonga illustrate the value of embedding Information and Communication Technology (ICT) preparedness in schools and developing youth-centered digital competencies tailored to both main islands and remote communities. Equipping communities with the skills to use digital tools during crises is essential for ensuring the effectiveness of early warning systems and humanitarian communication.

Resilience must also be grounded in rights-respecting governance. Early warning systems were consistently framed as a matter of human rights rather than mere service delivery. Data governance frameworks should mandate minimum data collection, clearly defined humanitarian data-sharing protocols, and safeguards that prevent individuals from having to trade privacy for safety. “Trust-by-design” approaches—centered on predictable, transparent information flows—were identified as more effective than punitive misinformation controls, particularly during emergencies when trust determines the reach and impact of crisis communication. Cross-border cooperation, such as bilateral data-sharing arrangements for disaster alerts, reinforces the need for regional standards that align humanitarian response with rights protection.

Community-driven innovation further strengthens infrastructure resilience. The Participatory Research and Ownership with Technology, Information and Change (PROTIC) II initiative in Bangladesh exemplifies how co-designed, locally relevant technologies—such as PAROLI, an offline voice-based communication platform—can function during power outages and network failures[24]. By enabling real-time community alerts, SOS signaling, and coordination "without the internet," such tools provide an alternative communication backbone during cyclones or floods. Similarly, digital inclusion initiatives for fisherfolk communities demonstrate how localised knowledge, early warning systems, and digital literacy can enhance safety, empower community advocacy, and preserve indigenous practices.

Sustained investment must underpin all resilience efforts. Governments should formally designate the Internet as critical infrastructure within national disaster and development frameworks. This designation should be supported by long-term financing mechanisms, sustainable infrastructure funds, and responsibility frameworks that ensure digital systems remain operational beyond the immediate aftermath of a crisis. Regional collaboration—through shared backup channels, coordinated drills, joint training, and mutual technical assistance—should be institutionalized to ensure that no country faces disruptions in isolation.

Infrastructure resilience in the Asia Pacific is therefore multidimensional. It requires robust physical infrastructure, equitable access, strong community capacity, rights-protective governance, and inclusive innovation. When these elements are integrated, digital systems evolve from fragile utilities into resilient lifelines capable of supporting communities before, during, and after disasters.

Resilience Against Regulatory Overreach

While infrastructure resilience ensures continuity, regulatory resilience safeguards openness and trust. Across many jurisdictions, regulatory attention has increasingly shifted toward imposing personal criminal or civil liability on platform executives and employees[25]. This trend represents a profound restructuring of platform governance, where responsibility for systemic failures is transferred from institutions to individuals. High-profile incidents — such as the arrest

[24] APrIGF 2025, "Experience of Co-designing Digital Justice and Inclusion Initiatives with Communities in Bangladesh". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2NzY1ZjIwM2FkMy8vMzkvLzIzODMvLzA= (last accessed 8 December 2025)
[25] APrIGF 2025, "The Growing Threat of Personal Liability in Platform Regulation: A Necessary Measure or Overreach?" Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2N2NmMTM0ZGUxNi8vMzkvLzI0MTAvLzA= (last accessed 8 December 2025)

of Telegram's founder and the suspension of X (formerly Twitter) in Brazil — illustrate how quickly governments may escalate enforcement measures, raising questions about proportionality, due process, and the long-term implications for digital freedom and innovation.

The evolution of intermediary liability frameworks provides essential context for this shift. Early Internet regulation, shaped by instruments such as the U.S. Section 230, the European Union (EU) E-Commerce Directive, and India's IT Act (2000), focused on enabling innovation and free expression by protecting intermediaries from liability for user-generated content. However, as platforms accumulated political, social, and economic influence — particularly following watershed events such as the Arab Spring, the Cambridge Analytica scandal, and the Christchurch attacks — governments began introducing stricter duties of care. Recent regulatory models, including the EU's Digital Services Act and the United Kingdom (UK)'s Online Safety Act, require proactive risk mitigation and greater transparency. Yet when adopted in the Global South, these mechanisms often morph into tools for punitive enforcement, with local compliance officers exposed to significant personal risk without adequate safeguards.

This regulatory environment intensifies existing structural challenges in platform governance. Many global platforms still lack sufficient local presence or transparent grievance mechanisms, allowing them to evade timely compliance or engagement with national authorities. Users, meanwhile, face slow or ineffective redress for harms ranging from harassment to misinformation. Automated moderation systems — often trained on Western-centric linguistic and cultural norms — routinely misclassify or overlook harmful content in under-resourced languages, reinforcing inequities and weakening trust. These gaps are compounded by jurisdictional evasions: for years, platforms headquartered abroad relied on foreign incorporation and U.S.-based governing law clauses to avoid accountability in domestic legal processes.

Efforts to correct this imbalance have included mandates requiring platforms to appoint local legal representatives and, in some cases, data localisation rules aimed at enhancing state oversight. While these measures can strengthen accountability and provide clearer channels for enforcement, they also create new risks. In environments with weak rule of law, local representatives may face intimidation, arrest, or political pressure. Requirements for in-country data storage can further enable surveillance, censorship, or abuses of state power under the guise of regulatory compliance.

Building resilience against regulatory overreach therefore requires a balanced, systemic approach. Personal liability should apply only in narrowly defined circumstances — such as clear complicity, willful negligence, or documented knowledge of wrongdoing — and must be supported by rigorous due-process safeguards. Broader accountability should be anchored in institutional mechanisms: meaningful fines with enforceable recovery processes, independent algorithmic audits, transparent reporting obligations, and cross-border regulatory cooperation.

Public oversight, including engagement from civil society and independent researchers, is essential to preventing misuse of regulatory authority. A resilient digital ecosystem is one where safety, innovation, and fundamental rights reinforce rather than undermine one another — and where accountability rests on robust governance frameworks, not on exposing individual employees to disproportionate and politically motivated risk.

Funding for Resilience

Strengthening digital resilience requires financing mechanisms that are adaptive, sustainable, and capable of addressing the full breadth of barriers that prevent individuals and communities from realising meaningful connectivity. Universal Service Funds (USFs) are government-mandated financial mechanisms designed to ensure that everyone—especially people in remote, rural, or underserved areas—can access essential telecommunications and Internet services. Unfortunately, the traditional model of USFs has not kept pace with the complexity of today's digital ecosystem. Its historic emphasis on expanding physical infrastructure has resulted in a narrow application of resources, leaving unresolved gaps in affordability, device access, local content availability, online safety, and the broader socio-technical conditions required for equitable digital participation[26].

Persistent under-utilisation of USF resources reflects structural constraints that include political and regulatory bottlenecks, outdated investment priorities, and subsidy distribution models that limit innovation. These limitations have highlighted the need for a fundamental reorientation of USFs toward a broader development-focused mandate. Recasting USFs as Digital Development Funds (DDFs) would enable governments to fund not just connectivity, but the essential layers that determine whether connectivity can translate into resilience—such as

[26] APrIGF 2025, "Rethinking Universal Service Funds in South Asia: Challenges, Impact, and the Road Ahead". Proposal form and session report available at: https://forms.for.asia/proposal/?proposalform=Njg2MmIwNjAzNWYxOC8yMzkyLzIzNTIyLzA= (last accessed 8 December 2025)

digital literacy, community-level capacity building, trusted digital environments, and access to relevant services and content.

A modern funding approach must also recognise the importance of supporting emerging technologies. Participants noted that continued investment in obsolete systems—such as 2G networks—impedes progress, as these technologies lack the capacity to support the data-driven services central to contemporary digital life. Digital Development Funds would be better positioned to support diverse and innovative connectivity models, particularly those that address the needs of underserved or geographically remote regions.

Reforms in subsidy allocation were also identified as critical to ensuring that public resources deliver long-term value. The current reliance on least-cost auctions, while fiscally efficient, often prioritises minimal cost over service quality, sustainability, and inclusiveness. A hybrid financing model—supported by an institutional framework that balances autonomy with accountability—would allow funding decisions to better reflect contextual realities. The Asia Pacific Network Information Centre (APNIC) Foundation's work in developing such a framework demonstrates how structured governance can enable more strategic and transparent allocation of resources.

Achieving effective and equitable utilisation of funds requires the removal of systemic barriers that limit deployment of interventions. This includes improving institutional governance, strengthening transparency in fund management, and embedding comprehensive digital development goals—ranging from device accessibility to local content production—into funding mandates. Transitioning from USFs to Digital Development Funds would not only modernise the financial architecture supporting digital access but would also place governments in a stronger position to build resilient digital ecosystems capable of withstanding environmental, economic, and geopolitical shocks.

Through this transformation, funding mechanisms can evolve from infrastructure-centric instruments into holistic development tools, ensuring that investments in connectivity contribute directly to inclusion, empowerment, and long-term resilience across the region.

Annex I Regional Parliamentary Track Discussion Summary*

Navigating the Net: An Introduction to the Internet Ecosystem

The first session of the regional Parliamentary Track invited technical community representatives to introduce the Internet ecosystem and raise awareness regarding unintended consequences of regulation on the proper functioning of the Internet. The panel distilled concrete do's for drafting digital policy, which include to keep laws tech-neutral and flexible so they do not age out; to "think global, add local" by aligning national rules with the globally coordinated names-and-numbers system – Internet Corporation for Assigned Names and Numbers (ICANN) / Regional Internet Registries (RIRs) – to avoid splintering the Internet; to consult operators and the technical community early through multistakeholder processes to surface operational realities; to balance privacy with accountability so cybersecurity responders can reach the right network contacts lawfully and quickly; and to bake in open standards—notably IPv6, Domain Name System Security Extensions (DNSSEC), and Resource Public Key Infrastructure (RPKI)—to future-proof networks, Internet of Things (IoT), and smart-city ambitions. Finally, the panel encouraged the audience to build state capacity, equip staff regulators with real expertise and use sandboxes.

It was further suggested that legislators can immediately leverage the Asia Pacific (APAC) community by engaging beyond the parliamentary track, by attending main Internet Governance Forum (IGF) sessions, Asia Pacific Network Information Centre (APNIC) open policy meetings, ICANN/ Internet Engineering Task Force (IETF) fora, and draw on IGF and APrIGF outcome documents when legislative committees need cross-stakeholder policy advice.

Finally, they can invite registries/RIRs and network operators to hearings for briefings, borrow peer models via regional parliamentary networks, and request targeted technical training from DotAsia/APNIC.

This ecosystem gives lawmakers rapid access to comparative practice, real-world impact tests, and draftable language that travels well across borders.

Practical guidance for lawmakers

- **Think global, add local**: align national laws with globally coordinated systems for names/numbers; avoid rules that conflict with RIR/ICANN policies.
- **Consult early & often**: run multistakeholder consultations with operators, civil society organisations (CSOs), standards bodies, and RIRs to surface operational realities.
- **Be tech-neutral & flexible**: write principles-based provisions that won't be obsolete as technologies evolve; consider sandboxes.
- **Balance privacy & security**: enable lawful, timely access to operational data for cybersecurity while protecting personal data.
- **Promote open standards**: explicitly support IPv6, DNSSEC, RPKI, and other widely recognized best practices.
- **Build state capacity**: staff regulators with strong networking/cyber expertise and support their participation in IGF/APNIC/IETF fora.
- **Leverage IGF assets**: use IGF messages, APrIGF Synthesis Documents**,** and Parliamentary Track outputs as reference material for committees.

How can Members of Parliament benefit from the community

- Network with peers (e.g., African Parliamentary Network on Internet Governance) to exchange models and text.
- Tap on technical training and briefings from .asia/APNIC and others; invite them to hearings and drafting sessions.
- Participate not only in parliamentary tracks but also main IGF program sessions to hear cross-stakeholder perspectives on pending bills.

Governing Digital Platforms in the Asia-Pacific: Strengthening Public Policy through Multistakeholder Insights

The second session of the regional Parliamentary Track on governing digital platforms in the Asia Pacific (APAC) urged lawmakers to govern platforms with transparent, rights-based, innovation-friendly rules. Key priorities were discussed to avoid fragmented, reactive laws, to

use multistakeholder consultation early (government, digital platforms, civil society, technical experts, youth), to balance safety with freedom of expression and economic growth, and to build state capacity so ministries can coordinate on cross-cutting platform issues.

Practical levers include requiring algorithmic accountability and transparency, promoting AI fairness and content-moderation safeguards that do not silence marginalised voices, and calibrating compliance so Small and Medium Enterprises (SMEs) are not crowded out.

Legislators were further encouraged to embed inclusion and accessibility by design, treating web/app accessibility as a baseline requirement, while pairing governance with digital literacy to curb mis- and disinformation and support safer participation.

Legislators can plug into the community by holding recurring national forums that bring together all stakeholder groups, with targeted tracks for under-heard groups (women, persons with disabilities, or from rural areas).

Practical guidance for lawmakers

- **Legislate tech-neutral, rights-based rules** for platforms that safeguard freedom of expression while enabling safety, competition, and innovation.
- **Institutionalize multistakeholder input early** (government, digital platforms, civil society, technical experts, youth) and keep it continuous.
- **Require platform accountability**: transparency reporting, notice-and-appeal for users, basic algorithmic transparency and impact assessments (with special attention to AI bias).
- **Bake in inclusion & accessibility by design**: make accessibility standards a baseline for public- and large-platform services; require inclusive user experience (UX) and language access.
- **Calibrate compliance to size/risk** so SMEs and startups are not crowded out (graduated duties, safe harbors, model templates).
- **Strengthen state capacity & coordination**: equip regulators and staff with networking/AI/content-moderation expertise; set up clear lead ministry and inter-ministerial coordination for cross-cutting issues.

- **Pair governance with digital literacy** programs to counter mis/disinformation and deepfakes, especially for vulnerable groups.
- **Promote open standards and interoperability** that support a resilient ecosystem and reduce lock-in.

**report received from the IGF Secretariat*

Appendix I

Name	Affiliations	Stakeholder Group
Shahanaj BEGUM	Individual	Technical Community
Zainab Fayyaz CHEEMA	Individual	Youth
Joyce CHEN	APNIC	Technical Community
Dr. Amrit CHHETRI	My Cyber Hubs	Technical Community
Amrita CHOUDHURY	CCAOI	Civil Society
Sharmin ISRAIL	Individual	Civil Society
Nguyen Thi Ngoc HUYEN	Students For Liberty APAC	Civil Society/Youth
Hino Samuel JOSE	Individual	Civil Society/Youth
Syed S. KAZI (Co-Chair)	Council for Social and Digital Development	Technical Community
Alban KWAN (Co-Chair)	Individual	Private Sector
Cheryl LANGDON-ORR	Internet Australia	Civil Society
Yuan-Ting LIN	National Communications Commission	Government
Elizabeth POLLARD	Individual	Youth
Winston ROBERTS	Individual	Civil Society
Om Prakash SHARMA	Individual	Youth
Ritu SRIVASTAVA	IEEE	Technical Community
Yien Chyn TAN (Co-Chair)	ICANN	Technical Community
Ashirwad TRIPATHY	Educating Nepal	Civil Society
Anika VASHISTH	Individual	Youth