

IGF 2025 Session Summary: Strengthening Multistakeholder Digital Cooperation

- IGF 2025 | Lillestrøm, Norway | 25 June (14:45 – 15:30)
- Organized by: Global Forum on Cyber Expertise (GFCE)
- Speakers:
 - Moderator: Klara Marland, Advisor, GFCE
 - Kenneth Pugh, Senator of Chile
 - David Fairchild, First Secretary, Permanent Mission of Canada, Global Affairs Canada
 - Rose Payne, Policy and Advocacy Lead, Global Partners Digital (GPD)
 - Francesca Bosco, Chief Strategy Officer, CyberPeace Institute (CPI)

Session Overview

This session explored how diverse stakeholder groups — including civil society, academia, the technical community, and the private sector — can be meaningfully involved in shaping the future UN Permanent Mechanism on ICT Security. Discussions focused on operationalising inclusion, ensuring continuity of engagement, and building sustainable structures for stakeholder participation beyond symbolic involvement.

Guiding Questions

- What role should nonprofits and civil society play in the future UN Permanent Mechanism, and what would that look like in practice?
- How can underrepresented voices be meaningfully included?
- What strategies can ensure that multistakeholder input is continuous and not ad hoc?
- Are there international processes that offer good models for stakeholder engagement?

Key Themes and Insights

Government Perspectives: Enabling Structural Inclusion

- **Examples from Chile** highlighted efforts to institutionalise trust and multistakeholder collaboration through national frameworks:
 - A permanent public-private advisory committee.
 - Legal protections for ethical hackers.
 - A national Cybersecurity Month to raise awareness and foster dialogue.
- **Canadian approaches** reflected sustained advocacy for stakeholder inclusion in UN-level cyber processes. This includes:
 - Co-authored proposals for inclusive modalities in future mechanisms.

- Support for multistakeholder participation through sustained partnerships and funding.
- Recognition of cyberspace's inherently multistakeholder "DNA", reinforcing the need for diverse inputs to strengthen norm implementation and capacity-building efforts.

Civil Society Contributions: Operational Value and Practical Challenges

- Stakeholders were recognised as critical to enhancing legitimacy, bridging geopolitical divides, and ensuring cyber policies are relevant and locally informed.
- Tools and initiatives developed by civil society — such as cyber incident tracking platforms and nonprofit cybersecurity providers — demonstrate tangible impact.
- Challenges persist, including:
 - Restrictive accreditation processes.
 - Inadequate and unsustainable funding.
 - Barriers to ECOSOC accreditation for technically proficient organisations.

Reflections on Inclusion

- There was wide agreement that stakeholder participation must go beyond thematic or symbolic consultation. Key recommendations included:
 - Transparency in decision-making processes, especially around accreditation and objections.
 - Public visibility of stakeholder inputs and traceability of their impact.
 - Rolling, asynchronous opportunities to contribute — enabling meaningful engagement beyond rigid time slots.

Q&A and Interactive Discussion Highlights

- **Youth representatives** questioned whether stakeholder models are inclusive or self-selecting. The discussion acknowledged structural inequities, such as accreditation restrictions and high participation costs that disproportionately affect less-resourced actors.
- **Examples from practice** illustrated how hybrid participation models, early sharing of agendas, and inclusive funding mechanisms can help counterbalance power imbalances — especially at national levels where governmental dominance is often more pronounced.
- A **civil society tool** addressing non-consensual image sharing (StopNCII.org) was presented as an example of a survivor-centric initiative that could be integrated into broader cyber policy frameworks.
- **Questions on power imbalances** and stakeholder influence sparked calls for capacity-building to be prioritised alongside participation, ensuring both presence and capability.

Emerging Recommendations

1. **Institutional Reforms:** Move from invitation-based models to inclusive, structural mechanisms for stakeholder involvement.
2. **Hybrid Participation:** Enable meaningful engagement through virtual access, rolling interventions, and early release of documents.
3. **Funding and Accessibility:** Support underrepresented groups through travel funding, remote access, and long-term capacity-building support.
4. **Transparency:** Improve clarity around accreditation, objections, and the use of stakeholder contributions in decision-making processes.
5. **Coalition Building:** Encourage stakeholder coalitions—by theme or region—to strengthen coordination and amplify diverse voices in global cyber diplomacy.

Conclusion

The session underscored the need for a more equitable, transparent, and sustainable multistakeholder approach to digital cooperation, one that recognises stakeholders not merely as contributors, but as essential partners in building a secure and inclusive cyberspace.