

Yrjö Länsipuro, Salla Toiviainen
28 November 2025

Finnish Internet Forum 2025

Finnish Internet Forum 2025 was held 8 October in the Auditorium of the Annex to the Parliament House in Helsinki. Main themes of this year's FIF were resilience of digital infrastructure, cyber harassment and the 20-year review process of the implementation of the outcomes of the World Summit on Information Society (WSIS). The Forum had about 70 on-site and 200 online participants, including members and staff of the Committee for the Future, which had listed FIF as a regular open committee meeting on its calendar. The overall moderator of the Forum was Janne Hirvonen, Counsellor from the Department for International Trade of the Ministry for Foreign Affairs, coordinator of the FIF organizing group.

How to protect the infrastructure that our digital everyday life is based on, how to tackle digital harassment on the net? This year's Forum had to focus more on threats rather than opportunities. However, that was somewhat balanced by the third theme of the conference, WSIS+20 and its efforts to preserve for the future the best of two decades of the follow-up.



Finnish Internet Forum, the Finnish national IGF, has since 2010 been organized by a wide array of stakeholders, among which the Ministry for Foreign Affairs and the Finnish Internet Association (ISOC Finland Chapter) have been the most consistently engaged, in partnership with the Committee for the Future of the Parliament, which again made it

possible for the forum to meet in the auditorium of the Annex of the Parliament (“Little Parliament”)

The 2025 forum was opened by the Vice-Chair of the committee, Timo Harakka (MP-Social Democrats), who highlighted its role in enabling people to make the choices and decisions about the future, rather than just reacting to the development of technology. “Has the planet been harnessed to the needs of AI, or can we make the AI to serve the planet?”

In his opening remarks, Antti Vasara, the MFA special envoy on international technology policy, warned about the dangers of digital authoritarianism, and called for sharper awareness of the spread of surveillance systems, censorship, and the use of technology for social control. “Finland is known for its strong digital competence and open society. We have an opportunity to lead the way not only in the development of technology, but also in its regulation in an ethical and people-centered way”, he said.

In his keynote speech, Kurt “Kurtis” Lindqvist, President and CEO of ICANN since December 2024, returned to the times when he set up the first ISP in Åland, an autonomous province of Finland. In his speech, there was a clear line from those pioneering times to the present, when the Internet, despite its enormous expansion, still works well because “nobody owns, directs or controls” it. Internet is not about power, it is about cooperation, he said and warned about the efforts by “some countries” to centralize its governance in a way that may lead to fragmentation.

1st Panel: Resilience of Critical Digital Infrastructure

Resilience of digital infrastructure, a hot topic in Finland after various incidents in recent months, was the theme of first panel. It was introduced by the moderator Julf Helsingius, Chair of the Board of Base N and member of the Board of ISOC Finland. He noted that to a certain extent, internet has resilience built in, but it has its limits that are being tested today.

Kurtis Lindqvist agreed that malicious attacks against the physical infrastructure are getting attention now, but policy decisions that fragment the internet may be equally dangerous. “We can have an internet the most resilient physical infrastructure, but if it then starts fragmenting, the harm can be worse than that from cutting sea cables, and it is easier to do,” he said and stressed the need to ensure the resilience of all layers of the internet.

Olli Peltonen, Commander (Ret.), Finnish Navy and senior consultant at COPOY, explained Finland’s dependence on sea cables in the Baltic for its international connectivity. Their location is public knowledge, and they are easy soft targets for malicious action, something that he saw behind recent incidents on the Gulf of Finland when ships had damaged cable by dragging their anchors on the seabed. “We are being tested”, he warned. In spite of apparent redundancy, we need to prepare for worst case

scenario. That means increasing the capacity for cable repairs, eg. by adding such capabilities to the Finnish icebreaker fleet, and rehearsing rerouting of communications.

Elina Ussa, the CEO of FICOM, started with a simple fact: If networks fail, society ceases to exist. The priorities in Ukraine have been clear: keeping the country connected, no matter what. She encapsulated her recommendations in three points: 1) In a crisis, no operator or public authority can make it alone, mutual trust and cooperation are a must, 2) Clear and predictable regulation; in a crisis, there is not time for lawyers to debate, what a paragraph means; 3) Training and practice: resilience can't be legislated, it must be trained and tested. In Ukraine, national roaming became the lifeline, because operators had trained opening their networks to each other.

Maria Rautavirta, Head of Data Policy at the Ministry of Transport and Communications agreed that the core of resiliency is not isolation, but switchability within a flexible structure, comparable to that of the internet itself. She noted that platforms had captured a large part of tasks that belonged to society, but now the European Union was working to get them back.

Christiane Kirketerp de Viron, Deputy Director-General (Digital Society, Trust and Cybersecurity), of DG CONNECT, European Commission, participating remotely from Brussels, had the last word on this panel. She stated that resilience of European critical infrastructures has never been more relevant than now, when it is under continuing attacks in various ways. She also stressed the need of cooperation between public and private sector, and among all stakeholders, in implementing the robust policy structures now in place to defend the European critical infrastructures (NIST-2, Cyber resilience act etc.)

2nd Panel: Tackling Online Harassment – Steps Toward a Safer Internet

The second panel was about tackling cyber harassment and making the Internet safer, moderated by Oona Kurppa, Chair of Generation Equality and introduced by Reetta Hänninen, Leading expert at Sua varten somessa, an award-winning non-profit that operates on social media platforms to support youth aged eight to 21 years. She presented shocking survey results: 80% of young people had seen harassment on the internet, 40% had been its target. Digital harassment has become part and parcel of school bullying and other forms of abuse experienced by young people. Of young people between 11 – 17 years, 31% have received grooming attempts by adults. Of those targeted, 60 % don't tell anybody about their experiences, and those who do, tell friends and not adults. Authorities become aware of only 10 %.

Ella Granström, anti-violence expert from Women's line stated that digital harassment is also part of the experience for the women that seek help from her organization. It exacerbates their fears and anxieties and leaves them feeling hopelessly alone. For anybody trying to meet and help the women, the key is to believe them and not to downplay the trauma they have experienced.

Minna Kröger, Corporate Responsibility Director of Elisa described the operator´s profound and proactive approach to the problem by promoting the digital skills of Finnish children through its digital schools. Starting from the age of 7, children get to practice the basics of digital security and discuss their own safety online.

Atte Harjanne (MP – Green Party) noted that while the development of the Internet has lowered the threshold for digital harassment, the means at the disposal of the state to cope with the situation have not been scaled up accordingly. He urged platforms to take the problems seriously, and called for a culture that does not leave young people alone with their bad experiences.

Minna Kröger agreed with the point and commented that according to Elisa´s surveys, only 4 % of the children who experience digital harassment feel that they can discuss it with a safe adult.

To the moderator´s question about the awareness of the problem and willingness to do something about it among MP´s, Atte Harjanne replied that since the Internet presents a different face to each user, it may be difficult to MP´s to understand the use experience of children. That´s why it is useful to hear about the problems directly from children and young people, and not to try to dictate solutions over their heads.



All panelists agreed that even though children and young people, girls and women, and various vulnerable and visible groups are most prone to digital harassment, it can also be a threat to the democratic society as a whole, because it is so easy, and because technical development – like AI - is making it worse.

A suggestion from the floor: as an analogy from urban traffic, “pedestrian crossings” should be provided by platforms as safe, harassment-free areas.

Discussion Session: Is WSIS+20 still relevant?

The last item of the day was WSIS+20, especially the future role of the Internet Governance Forum, which is going to be decided by the UN General Assembly by the end of the year. It was moderated by Mervi Kultamaa, counselor at MFA and member of the Board of ISOC Finland chapter.

Miapetra Kumpula-Natri (MP – Social Democrats), who earlier as a Member of the European Parliament participated in the parliamentary track sessions of many IGF's, related her experiences and came with critical remarks and suggestions for how to improve the conference whose sheer size and huge selection of different topics make it problematic. Janne Hirvonen noted that the IGF is only the apex of a large system that has grown to include some 170 regional and national fora, including the Finnish one.

Closing remarks, with a succinct summary of the important points of the day's proceedings, were presented by Kirsi Karlamaa, technology and strategy director of Traficom.