IGF's Best Practice Forum on Cybersecurity contributes to intersessional consultative meeting of the UN's Open-Ended Working Group

New York, 3 December 2019 - The IGF Best Practice Forum on Cybersecurity presented its work at the United Nations' Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. The OEWG held its informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia on 2 - 4 December 2019 in New York at the UN headquarters.

The Best Practice Forum (BPF) Cybersecurity is one of the core intersessional activities of the Internet Governance Forum (IGF) initiated since 2014. The most recent work track of the BPF identified spaces of norms development across the community, analysed 19 cybersecurity agreements and collected best practices on how signatories put these agreements into practice. The *Paris Call for Trust and Security in Cyberspace* and the *UNGGE* 2015 consensus report are two such examples. The BPF observed convergence points of different norm proposals and early signs of consensus on what is proper behaviour in cyberspace, identifying potential in developing foundations for further work. This process, however, requires the creativity that only multistakeholder and multidisciplinary collaboration can bring to debate and fruition.

BPF Cybersecurity Lead-expert Maarten Van Horenbeeck highlighted some key findings disseminated at the 14th Meeting of the IGF, held in Berlin from 25 to 29 November 2019:

- Ongoing discussions on content online are meaningfully different to discussions on cybersecurity and conflating both can limit progress on one or the other.
- Cybersecurity agreements have positive outcomes. For instance, the inclusion of all stakeholder groups in the creation of agreements reinforces the shared nature of the challenge and builds agreement around the responsibilities all have.
- Cybersecurity agreements may have adverse effects. For instance, cybersecurity agreements are at risk of becoming counterproductive when they fail to focus on outcomes and instead prescribe a course of action; and cybersecurity agreements sometimes undermine human rights, which, in turn, may reduce cybersecurity.
- The quality of cybersecurity agreements can be improved, for instance, by defining key terminology early; by avoiding needless ambiguity through multi-stakeholder inclusion in reviewing language; and by making capacity building a crucial part of any agreement.

Several participants at the OEWG consultation emphasized the need for spaces for different processes and stakeholder groups to convene and discuss and acknowledged the IGF and BPF Cybersecurity as one of the places well suited for such exchanges.

More on the IGF BPF on Cybersecurity

Contact: bpf-cybersecurity-info@intgovforum.org / igf@un.org

BPF on Cybersecurity webpage and report
The BPF on Cybersecurity presented its draft report at the IGF 2019 (Berlin, 25-29 Nov.) and is now in the process of incorporating additional insights from that discussion in its final report: https://www.intgovforum.org/multilingual/content/bpf-cybersecurity

Full text of the IGF BPF on Cybersecurity Contribution to the OEWG: https://www.intgovforum.org/multilingual/filedepot_download/8395/1825