Empowering global cooperation on cybersecurity for sustainable development and peace

Messages

- Cybersecurity and the preservation of a secure and reliable cyberspace are essential elements in the road towards sustainable development. Some pointed out that countries have different levels of preparedness to deal with cyber threats and cyber risks, and more efforts need to be focused on capacity building measures. It is important for countries to have institutions, strategies, and policies in place to tackle cybersecurity issues, but capacity development should also focus on individuals.
- Cybersecurity cannot be achieved by one stakeholder group on its own, and all stakeholders have roles and responsibilities. Participants warned that siloed approaches can lead to ineffective and counterproductive measures, multistakeholder cooperation needs to be reinforced. Such cooperation carries challenges, one of them being related to the fact that there is no universally agreed definition of cybersecurity. Hence, a global culture of cybersecurity could help to enhance mutual understanding among stakeholders on what, when, how can be done to ensure an open, secure, stable, and accessible cyberspace.
- While there was broad agreement that international law applies to cyberspace, calls were made for more efforts to clarify how it applies, and to identify whether there might be gaps in some areas that international law does not cover.
- Participants shared the view that cyberspace should be a place for peace, stability, and prosperity. International cooperation among states, some suggested in the framework of the UN, could contribute to avoiding a cyber arms race and militarisation of cyberspace.
- Many agreed that existing norms related to responsible state behaviour in cyberspace – although not binding – can significantly contribute to enhancing cybersecurity and stability. Calls were made for more awareness raising about these norms, and more efforts to enhance their voluntary implementation.
- While some called for new international treaties or convention to encode rules, norms, and principles for cybersecurity and responsible state behaviour, others considered this premature and called for first identifying what could be the mechanisms that would allow meaningful engagement of all stakeholders in the development of rules. Moreover, questions were raised on the actual implementation and effectiveness of any potential future international agreement considering that there is still lack of clarity on how existing international law applies to the use of digital technologies by states.