Open-ended Working Group on developments in the field of information and telecommunications in the context of international security
Second substantive session
New York, 10-14 February 2020 UN Headquarters

Speaking notes (as delivered)

Thank you, Chair.

The discussions for the past few days have been thought-provoking, forward-looking, and highly energized. As also acknowledged by many delegates, we believe that the Group will achieve concrete outcomes in its forthcoming report under the leadership of the Chair with the strong support of fellow secretariat colleagues.

While there are issues of divergence - understandably, given the complexity in this diverse field of ICT in international security context - there are also issues of convergence, with useful proposals raised by, and built upon, by delegates here.

One issue of convergence is on the need to increase awareness, and to enhance understanding of the agreed 11 norms of responsible state behaviour that were part of the 2015 GGE report, as endorsed by the General Assembly.

We also heard repeated calls for states to operationalize these agreed norms, and to share lessons learned, underscoring the important linkage between norms and capacity development.

And for capacity development to address the needs and gaps-- not just for government actors, but also non-government actors, including civil society, private sector, and the Internet technical community that own respective roles and responsibilities in managing the global critical Internet resources.

The needs for capacity development have been articulated eloquently by many distinguished delegates here.

Along these lines, I would like to draw your attention to the work of the Internet Governance Forum – or the IGF in short - and how the IGF could contribute to the work of this Group.

As a global forum for multistakeholder policy dialogue on the Internet, the IGF has been convened by the Secretary General since 2006, supported by the UN Department of Economic and Social Affairs, UN DESA, through the IGF Secretariat.

As a platform for discussions, the IGF brings various stakeholder groups to the table as equals to exchange information and share good policies and practices relating to the Internet and digital technologies.

While the IGF may not have decision-making mandates, it informs and inspires those who do.

The IGF also acts as a global capacity development platform, as it facilitates common understandings and knowledge exchange of stakeholders from all countries, paying particular attention to developing countries -- not only on how to maximize opportunities brought about by the Internet, but also addressing risks and challenges.

Between the annual meetings of IGF, there is robust intersessional works that involves experts, practitioners and other stakeholders in an open inclusive manner

Since the IGF convened its first annual meeting in 2006, Security has been a key theme of its work.

Over time, concerns about cybersecurity have – quite rightly – increased. And these escalations have been reflected in the focus of the IGF.

At its most recent meeting in Berlin, with gratitude to the Government of Germany as the host country, cybersecurity issues were prioritized under the key thematic track of 'Security, Safety, Stability and Resilience'. The other 2 main themes were data governance and digital inclusion.

The Berlin IGF Messages have emerged as a key outcome of the IGF. They captured the main policy messages that emanated during the Berlin IGF and its intersessional activities, many of which touch upon issues directly related to the discussions of the Group here.

The IGF Messages underline the importance of cybersecurity norms as well as norms development, and stress that 'every effort to pursue what is considered proper behaviour contributes to establishing community-wide supported cybersecurity norms.'

The IGF messages also underline that 'discussions on online safety need to rely on robust data', and that the 'international multistakeholder community needs to accurately define scope and terminology' and develop a 'shared understanding amongst all players' as a basis for agreement on ways to act and cooperate.

The complete sets of IGF Messages are available on the IGF website.

The IGF's Best Practice Forum on Cybersecurity, an intersessional multistakeholder activity established in 2014, gathers best practices on cybersecurity. During its 2019 work cycle, it focussed on international cybersecurity norms and agreements, reviewing 19 cybersecurity initiatives and identified best practices on how signatories put their commitments into actions. This analysis included the Paris Call for Trust and Security in Cyberspace and the UNGGE 2015 consensus report.

Some key learning points are:

As threats in cyberspace are becoming more commonplace and severe, cybersecurity norms and agreements provide a valuable common footing to reduce risk and increase security and stability in cyberspace.

While the relevance of such norms and agreements have been underscored by many delegates in this discussion, there is also risk that they may become ineffective or even provoke adverse and counterproductive effects, especially when they:

- limit multistakeholder input;
- fail to focus on outcomes but instead prescribe a particular course of action;
- miss the involvement of important global players;
- lack leadership in implementation;
- directly or indirectly undermine human rights, which in turn may reduce cybersecurity.

Distinguished Chair and delegates,

As Secretary-General António Guterres highlighted in his opening address at the Berlin IGF last November, the IGF could be a platform where government representatives from all parts of the world – along with companies, technical experts and civil society – can come together to share policy expertise, debate emerging technology issues, agree on some basic common principles, and take these ideas back to appropriate norm-setting fora.

The IGF could be one of the venues for capacity development and "institutional dialogue" for this Group -- a place to consult and have an open inclusive exchange with the stakeholder groups of the IGF, that include Governments, civil society, private sector, and the Internet technical community, as well as intergovernmental and international organizations.

This year, the 15th meeting of IGF will be hosted by the Government of Poland in November. This important work on security will continue.

The Best Practice Forum on Cybersecurity will continue its work on cybersecurity norms and agreements to map overlapping and initiative-specific commitments and to collect and exchange best practices on how stakeholders implement these commitments.

It will also identify methods of norms assessment as implemented by different stakeholder groups and plans a dialogue with experts from multidiscipline including social science where norms have been dominant forms of rulemaking to identify learnings that can be applied in cybersecurity.

We invite all delegates here, as well as any other stakeholders to join these discussions, as well as the annual meeting in Poland this November.

We have also shared a position paper that is now available on the OEWG website.

On behalf of UN DESA and the IGF Secretariat, thank you for the opportunity to address you today.