Multi-stakeholder meeting of the Open-ended Working Group

Possible Framing Questions

(A) Cyber threat landscape: Existing and emerging cyber threats: A view from Industry and Academia

- What are currently the most significant cyber threats, and how are these expected to change in the future?
- What are the main threats to critical infrastructure and critical information infrastructure?
- How does the malicious use of ICTs affect socio-economic development and, in particular, the digital economy?
- How do new technological developments, such as artificial intelligence and blockchain, alter the threats to the global ICT environment?

(B) Rules, laws and norms: Creating a cyber space based on rules, laws and norms: How can stakeholders support Governments

- How can stakeholders such as industry, civil society and academia contribute to the implementation of the voluntary non-binding norms of responsible State behaviour contained in the report of the 2015 Group of Governmental Experts[1]?
- How can all stakeholders including governments support each other in the responsible reporting of vulnerabilities and/or sharing of information on available remedies to protect ICT-dependent infrastructure?[2]
- As both multi-stakeholder initiatives and intergovernmental norms emphasize the need to ensure the integrity of the supply chain of ICT products, how can multi-stakeholder cooperation on the operationalization of these norms be enhanced?
- States have agreed that international law, and the UN Charter in particular, applies to the use of ICTs. Building on these recommendations, what additional perspectives can other stakeholders offer to the OEWG?

(C) Rules, laws and norms: Stakeholders' commitments to rules, norms and principles: Tech Accord, Charter of Trust, Global Transparency Initiative, Paris Call and beyond

[1] The 2015 GGE report is available through https://undocs.org/A/70/174

[2] Norm (j), contained in paragraph 13 of the 2015 GGE report state that "States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure"

- What are the commonalities between the different multi-stakeholder initiatives on cybersecurity, such as the Tech Accord, the Charter of Trust, the Global Transparency Initiative, the Paris Call and other initiatives, and the norms developed at the inter-governmental level?
- What synergies should be encouraged between intergovernmental and multi-stakeholder initiatives to prevent us going on separate paths?

(D) Confidence-building measures and capacity-building: Confidence-building between States and between States and the Private Sector

- How can all stakeholders contribute to the implementation of confidence-building measures?
- How can confidence-building measures be further developed at a technical level through cooperation?
- What confidence-building measures should be co-developed between the Public and Private Sector?

(E) Confidence-building measures and capacity-building. Engaging all stakeholders to enhance capacity-building efforts

- How can all stakeholders including States cooperate to promote capacity-building including awareness and education?
- How can the needs and resources for capacity-building be best aligned, with a view to promoting complementarities and avoiding duplication?
- What roles can different stakeholders including States play in the development of national ICT-security strategies?

(F) Conclusion: Ways forward on a multi-stakeholder approach

- What are the main benefits of regular multi-stakeholder dialogue on international ICT-security?
- What modalities for continued multi-stakeholder dialogue are most useful to the different stakeholders?
- What can be done do to ensure the views of relevant stakeholders from all regions are represented in future multi-stakeholder dialogue?