High-level Panel Follow-up Roundtable 4 – Global Commitment on Digital Trust and Security
Session 1: 10 December 2019, 8am-10am EST

Meeting Note

Recommendation 4. We recommend the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.

Champions
Government of Estonia, Government of The Netherlands, Government of Uruguay, Microsoft, UN Office of Disarmament Affairs, Office of the Special Adviser

Key Constituents
Government of France, Government of New Zealand, Government of Singapore, Government of Switzerland, Government of Bangladesh, Government of Finland, Government of Mexico, Government of Japan, Government of Kiribati, Government of Kenya, Government of Canada, GovTech Lab, The Future of Life Institute, Center for Strategic and International Studies (CSIS), Konrad-Adenauer-Stiftung (KAS), Internet Commission, World Health Organization (WHO), Facebook, World Economic Forum (WEF), Internet Society (ISOC), World Bank, IEEE, International Telecommunication Union (ITU), ICT4Peace, UNICRI, UN Secretary-General's Task Force on Digital Financing of the Sustainable Development Goals (DFTF), UN Office on Drugs and Crime

Opening Remarks

It was noted that recommendation four, which calls for the development of a Global Commitment on Digital Trust and Security, will be among the most challenging elements to the follow-up to the Highlevel Panel report but also offers great opportunity for progress on digital cooperation. As such, transparency, regional diversity, and multistakeholder engagement will be critical to success.

These Roundtables present an opportunity to build confidence in the digital space and mitigate some of the digital challenges and threats. This recommendation offers the potential for new achievement in the digital space, including universal agreement and multistakeholder engagement, which can help address broader digital trust and security issues. It will be critical that the owners and developers of the the technologies in question are included in this discussion.

It is the opinion of the Champions that the objective of this recommendation is to formulate a *universal* political commitment while taking note of the many existing agreements such as the Paris Call, the Christchurch Call, the Siemens' Charter of Trust and others, this Global Commitment can be built on language in pre-existing agreements.

Efforts will have to be made to ensure that there is no duplication of the GGE and OEWG processes.

Themes from Key Constituents

Support for OEWG and GGE: All constituents expressed an interest to avoid duplication with ongoing multilateral processes, noting that the Global Commitment can be built based on language agreed in past governmental processes and combined with other cyber trust and security documents.

Universal adoption: The challenge of past digital norms and agreements is that they were only for a specific constituent group, be it Governments, industry or civil society, or it was a selective group of only like-minded participants, this effort should seek universality. The Global Commitment should also make an effort to incorporate women, developing countries and other groups less involved in digital cooperation efforts.

Objective of the Global Commitment: Many constituents called for a commitment that moved the world toward a free, fair and secure cyberspace, especially for civilians. The name and language of the Commitment can be further discussed and doesn't need to be finalized immediately.

Building on existing work: There was a strong emphasis to avoid duplication of ongoing or past efforts. Many actors in this space, including civil society, the private sector and Governments, have been leading initiatives in the area of cyber trust and security for many decades and Recommendation 4 of the report should not seek to create a new process but should build on already agreed issues and language, existing initiatives.

Engagement with diverse actors: It was widely noted that this process afforded the opportunity to have more representative multistakeholder input from actors in the global south, especially civil society, academia and the private sector. There was agreement that additional private sector participation would be beneficial to these discussions, especially from the global south. Professional associations in the ICT space are also afforded a strong voice in these discussions and would prove a valuable channel for promoting a Global Commitment and provide it with additional industry credibility.

Regional dimensions: Global institutions, governments and private sector actors noted that there are unique regional dimensions to cyber trust and security and that the Global Commitment should provide a measure of flexibility for those differences.

Areas of disagreement/new discussion: Some actors proposed discussion on new thematic areas including trust and security in artificial intelligence, dis-information, hate speech, and political processes as well as discussions towards a new mechanism for attribution and new bodies both within and outside the UN system, though there was limited support among multistakeholder actors for these concepts and some participants objected to these ideas. There was also discussion of working towards global cyber standards, depending on the industry, though this would prove complex and beyond the scope of the Recommendation.

Synergy with Recommendation 2: Many actors noted that a Global Commitment on Digital Trust and Security would be best realized if there was also significant investment in capacity building for developing countries and business that operate there – potentially lining up with the recommendation for digital help desks from Recommendation 2.

Champions closing remarks:

Recognizing that the timeline for this work is short and that the Recommendation is ambitious, the champions will seek more specific input from the Key Constituents in the form of a questionnaire which will be circulated around the year-end. The questionnaire will also be better informed by the circulation of a digital commitment mapping which will also be circulated.

Consideration will be given for the coordination of an in-person meeting in the new year once feedback and analysis have been done.

Champions noted the complementarity of this exercise with the ongoing work of the UN First Committee bodies, though recognizing that the themes and participants for this process are wider, crossing all UN pillars, and having significant private sector and civil society application.

It was also noted that the traditional UN committee structures are being challenged in the digital age as many technology issues, including digital trust and security, have cross-sectoral and cross-committee impacts.

Next Steps:

- Champions will circulate the initial mapping exercise to all Key Constituents and will share the question survey before the end of the year.

- Feedback will be consolidated in January and discussion can be had about a second virtual roundtable for February or potentially the coordination of an in-person meeting.