Permanent Mission of Sweden
to the United Nations

May 19, 2023

Excellency,

Reference is made to our letters dated February 22 and March 20, 2023, providing further details on the informal consultations with Member States, observers, and stakeholders in the form of deep dives.

At the beginning of the deep dive, the topic will again be introduced by briefers selected for their technical expertise, keeping in view our commitment to inclusivity of different stakeholders and to equitable gender and geographical representation throughout the consultations. The briefers will be asked to set the stage and not to speak exclusively from the perspective of the organization they represent. The briefers confirmed for this deep dive are Laurie Richardson, Google VP for Trust and Safety and Maayan Ziv, founder and CEO of AccessNow.

The next deep dive is scheduled for Thursday May 25, 2023, starting at 3pm and ending at 6pm ET (New York time) on the theme of *Digital trust and security*. The meeting will be held in the Conference Room 1.

In order to facilitate participation, you can find attached the guiding question for the session. Member States will make statements through their delegates participating in-person in New York only. Interventions will be limited to three (3) minutes. The link will again be shared via edeleGATE in case representatives of Member States wish to observe the meeting remotely.

We invite Member States to share this letter with relevant Stakeholders in your respective country, whose remote participation will again be facilitated. Interested Stakeholder participants can register via this website: https://www.un.org/techenvoy/global-digital-compact/intergovernmental-process

Please accept, Excellency, the assurances of our highest consideration.

Anna Karin Eneström
Ambassador Permanent Representative
of Sweden to the United Nations

Claver Gatete
Ambassador Permanent Representative
of Rwanda to the United Nations

Annex

Guiding questions for deep dive on "Digital trust and security"

25 May 2023

1. Digital spaces and online platforms can be exploited by actors for financial, criminal, social, political, or malicious goals - to spread falsehood, violent and extreme content, perpetrate scams and other crimes, and manipulate online behaviors. Which collaborative measures undertaken by Governments, the private sector and civil society have proved effective in tackling such misuse so far? How can global digital cooperation strengthen their implementation?
2. Different jurisdictions apply different norms to online behaviors. Different online platforms apply different policies to similar online behaviors. How can Member States, the private sector and relevant stakeholders engage to define common frameworks to address the challenges to online safety?
3. Regarding mis/disinformation and online harm, what policies, frameworks and measures can be adopted by governments and companies to protect the integrity of public information and preserve civic spaces for public debate?
4. What digital cooperation measures, for example trust labels, audits, and certification schemes, can stakeholders consider promoting trust and safety for consumer products and services, including AI models? How can we enhance digital literacy skills and training so that people are empowered to protect themselves?