Key Issues discussed (5-8 bullet points)

- Cyber threats landscape for the NGOs in the Humanitarian and Development sectors (NGOs). Example of cyber-attacks include Funds raised to provide medical care are being stolen; Humanitarian actors are targeted for surveillance; Data of survivors of violence are sold online; Disinformation operations sow distrust about humanitarian NGOs.

- Challenges for NGO and the disruption of aid delivery. There is an urgent need to build NGO resilience against cyberattacks.

- Recommendations from the workshop guiding questions: What pre-incident and incident response actions and measures could be taken? How to strengthen the digital ecosystem?
  - Raise awareness on cyber threats.
  - Equip staff with skills and knowledge related to cyber security through in-person training, simulation exercises, demonstrations.
  - Promote technical measures such as Multifactor Authentication, cyber hygiene, restricting access to websites, cybersecurity certification.
  - Risk assessment, prevention and response plan
  - Collaboration between the National CSIRTs is the most effective way for incident-crisis communication.
  - NGOs need dedicated funding to cybersecurity practices –governments support?
  - Institutionalize cybersecurity in the humanitarian sector (such as what’s done with critical infrastructure)
  - Increase cooperation with private sector on training issues.
  - Improve legal and policy framework (these should be linked to liability modeling and risk-based approach)
Towards WSIS+20 and WSIS beyond 2025, please share your views on the emerging trends, challenges, achievements, and opportunities in the implementation of the WSIS Action Lines to date (5-8 bullets)

Advancing digital inclusion while safeguarding the security and integrity of people’s worldwide, is clearly an opportunity for WSIS. However greater and sustained action is needed as cyberattacks are growing in scale and frequency and the societal structures needed to foster the SDGs will be the victims. Cyber “insecurity” is impacting at the same time human security, economic stability and development potential more broadly. Recognising and facilitating the inclusion of cybersecurity capacity building with other development objectives is crucial.

- Advocate for respect and development of policies, laws and norms strengthening the protection of humanitarian actors.
- Strengthen understanding and capacity of various stakeholders from the international development and International Geneva diplomatic community to implement a Safe Digital Humanitarian space through presentations/briefings.
- Raise donors' awareness on the importance of prioritizing humanitarian cybersecurity.

Tangible outcomes (such as key achievements, announcements, launches, agreements, and commitments (3-5 bullet points)

- Introduction of and presentation of key achievements of the CyberPeace Builders: an operational hands-on corporate volunteering connecting cybersecurity experts to humanitarian NGOs: over 110 NGOs protecting people in 120 countries; +300 missions and over 700 hours of cybersecurity support; +350 Volunteers provided by 30 different partner corporations.
- Sharing the announcement of the Humanitarian Cybersecurity Center launched on 27 February 2023 by the CyberPeace Institute and that provides free expert support and practical assistance to NGOs in the humanitarian and development sectors, tailored to their needs, and available anywhere in the world.

Actionable plan (2-5 points)

- Outcomes of the workshop will help reinforce existing mechanisms of the CyberPeace Builders to help strengthen the resilience of NGOs
• Pilot the design of relevant humanitarian cybersecurity tools, products and services that are vital to strengthen the resilience of all actors involved in humanitarian and human rights efforts. These will be effective through the Humanitarian Cybersecurity Center

Suggestions for thematic aspects that might be included in the WSIS Forum 2024 (WSIS+20 Forum High-Level Event) (one paragraph)

  o Technical and normative framework to strengthen the protection of humanitarian actors
  o Global Partnership for Sustainable Development: partnerships to build cyber resilience and security for vulnerable communities
  o Ethical dimensions the Information Society: Surveillance technology and impact on human rights