WSIS FORUM 19-23 MARCH 2018
Geneva | Switzerland

WSIS Forum 2018 OUTCOME DOCUMENT

Template for Submission of Executive Summaries for

Thematic/Country Workshop/ Action Line Facilitation Meetings/ Interactive Sessions/ High Level Dialogues/Publication Releases/Briefings

Deadline: Thursday 22 March, 2018

Exception: For sessions on Friday 23 March, please send at the latest 2 hours after the session

Please note that the WSIS Forum 2018 Outcome Document will be released on the ***23rd of March*** *(the last day of the Forum)*

1) **Title of your session**
   How to set the standard for cyber security? Guidelines and good practices.

2) **Name of Organization/s organizing the session**
   Global Forum on Cyber Expertise (GFCE)

3) **Relevance with the WSIS Action Lines – please specify the Action lines C1 to C11**
   C4 Capacity Building

4) **Key achievements, announcements, launches, agreements, and commitments (these will be reflected in the press release and Outcomes Document of the WSIS Forum 2018)**
   - Call for action from the GFCE to cooperate on a global level on the implementation of cyber capacity building.
   - Open call for GFCE Advisory Board Members! The GFCE is looking for representatives from academia, tech community or civil society. Deadline is April 1st.
   - Announcement to join the 'Triple I' (Internet Infrastructure Initiative) upcoming events to increase awareness on how to create robust, resilient and open internet infrastructure.

5) **Main outcomes highlighting the following:**
   I. **Debated Issues**
   - The main issues debated were how do we identify good practices? How do we make sure that these good practices get implemented?
   - The session started with an introduction by Manon van Tienhoven of the Global Forum on Cyber Expertise and its work as international multistakeholder platform where best practices and expertise is exchanged on cyber capacity building. The GFCE is moving

towards implementation of cyber capacity building, however more is needed than just good practices and guidelines. It is essential to identify the guidelines and good practices, the next step is to examine whether these guidelines and good practices are actually working or will continue to work under different circumstances, such as in a differerent environment or with different technologies. Only by cooperation lessons learned can be shared and explored with the GFCE community to facilitate the multistakeholder dialogue on cyber capacity building. Dejan Dincic from DiploFoundation explained on the process of identifying global good practices from the GFCE initiatives, a process that took place in 2017. He emphasized the comprehensive approach that is needed when implementing the good practices. A regional, decentralized approach is essential to succesfully implement good practices in different regions.

- Maarten Bottermanm represented the GFCE Internet Infrastructure Initiative and explained how a robust, open and resilient internet infrastructure is key to counter infringements and threats to the cyber domain. The initiative has developed global good practices, and the next step is to organize regional meetings to share these to bring together regional stakeholders and to raise awareness on Open Internet Tools.
- A regional example was provided by Abdullah Al-Balushi from the Information Technology Authority of Oman. In his presentation, he explained about Oman’s experience and achievements in the field of cyber security. He focused on the Oman eGoverment Architecture Framework , which is a set of standards/best practices and process management systems to enhance government services delivery. He underlined the importance of the multi-stakeholder approach, specifically the involvement of the private sector.
- The key question of the audience, which led to an interesting discussion, was: *Standards are a means to increase cyber security. When you look at the actors involved today, is the government really the actor with the strongest cyber security?* The main conclusion was that awareness on every level is key for strong cyber security. An interesting analogy was made by Dejan Dincic, with traffic. The government plays an important role, but you cannot (are not allowed) to drive a car as citizen, if you do not have a licence. Awareness at the end-user level must be raised to strengthen cyber security. The GFCE is starting multiple Working Groups, also on Culture and Skills, where awareness raising in a priority topic.

II. Quotes

- "Help make the Internet more reliable in your region: take action" **–** Maarten Botterman, representative of the Internet Infrastructure Initiative
- "Only by cooperation lessons learned can be shared and explored with the GFCE and the broader community to facilitate the multistakeholder dialogue on the implementation of cyber capacity building." – Manon van Tienhoven, GFCE Secretariat

III. Overall outcomes of the session highlighting

- Cooperation and a multi-stakeholder approach is necessary for successful global good practices and guidelines.
- Although cyber and the internet are global issues, cyber capacity building (WSIS Action Line C4) cannot be achieved with an one-size-fits-all approach.

IV. Main linkages with the SDGs

- SDG 8: Decent work and economic growth – Cyber capacity building increases economic welfare by enhancing e.g. e-commerce, as well as, by a safe digital environment.
- SDG 9: Industry, innovation and infrastructure – Cyber capacity building is key for safe industries and infrastructure, therefore also innovation, e.g. Critical Information Infrastructure Protection or CERTs.
- SDG 16: Peace, Justice, and strong institutions – Cyber capacity building can only be successful globally and contribute to developing international norms for cyber security and therefore keeps cyberspace stable.

V. Emerging Trends related to WSIS Action Lines identified during the meeting

A focus on the younger generation and volunteers based on trust instead of formal institutionalized mechanisms.

VI. Suggestions for Thematic Aspects that might be included in the WSIS Forum 2019

Focus on Skills and Awareness thematic workshop – which is key for cyber capacity building and cyber security in general - GFCE is interested in hosting such a workshop next year.

Please complete this document and send to Matthew L. Greenspan, Matthew.Greenspan@itu.int AND Gitanjali Sah, Gitanjali.Sah@itu.int