IGF 2017 Reporting Template

- Session Title: A Global Agenda on Cyber Capacity Building: Outcome GCCS2017 (OF69)

- Date: 20 December 2017

- Time: 16:15-17:15

- Session Organizer: Global Forum on Cyber Expertise Secretariat

- Chair/Moderator: Marjo Baayen, Deputy Head, GFCE Secretariat

- Rapporteur/Notetaker: Manon van Tienhoven, Advisor, GFCE Secretariat

- List of Speakers and their institutional affiliations:
    - David van Duren, Head of GFCE Secretariat
    - Carmen Gonsalves, GFCE co-chair Netherlands
    - Vladimir Radunovic, GFCE Advisory Board member / Director of e-diplomacy and cybersecurity programmes DiploFoundation
    - Paul Nicholas, Senior Director, Global Security Strategy and Diplomacy, Microsoft
    - Robert Collett, UK Foreign and Commonwealth Office
    - Lea Kaspar, GFCE Advisory Board co-chair / Executive Global Partners Digital (GPD)
    - Arnold van Rhijn, Netherlands Ministry of Economic Affairs and Climate Policy

- Key Issues raised (1 sentence per issue):
    - **Global Forum on Cyber Expertise (GFCE)** - in the GFCE over 60 organizations and states work together on practical initiatives to strengthen global cyber capacity building.
    - **Global Agenda for Cyber Capacity Building (GACCB)** – the GACCB was presented by the GFCE during the Global Conference on Cyberspace 2017 to strengthen international cooperation by developing a common (global) focus on cyber capacity building.
    - **GFCE Global Good Practices -** The capacity building work done in recent years by GFCE members and partners, both within these initiatives and beyond, provides a rich set of experiences and knowledge. Collecting and sharing GGPs will ensure that other cyber capacity building initiatives can benefit from this experience and expertise in their own efforts.
    - **Delhi Communiqué** – the Global Agenda was shared with the wider community by means of the *Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building*. In this document the structure and priorities of the Global Agenda were presented.
    - **Implementation of cyber capacity building** – in 2018, an Actionplan will be developed based on the Global Agenda to provide direction to the implementation of cyber capacity building.
    - **Multistakeholderism** – it is essential that all stakeholders work together on cyber capacity building.

- If there were presentations during the session, please provide a 1-paragraph summary for each presentation: No presentation available

- Please describe the Discussions that took place during the workshop session (3 paragraphs):
    - The Global Forum on Cyber Expertise (GFCE) has developed the Global Agenda for Cyber Capacity Building as an instrument to strengthen international cooperation, and ensure the use of common resources. In addition, the GFCE has prepared a set of Global Good Practices (GGPs). These GGPs are a number of hands-on results and practices developed by the different stakeholders in GFCE initiatives. This process was facilitated by DiploFoundation. Several of the Global Good Practices were explained in the panel, e.g. tools for testing the application of existing Internet standards in web services.

- On top of that, the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building was endorsed by over 60 members at the Global Conference on Cyberspace (GCCS) in Delhi in November 2017, highlighting existing principles as guidelines for capacity building (including broader ones such as the applicability of international humanitarian law to cyberspace, and respect of human rights online). In 2018, the GFCE is preparing to implement the Global Agenda. The importance of such a document was highlighted since it is easy to talk about capacity building, but experience learns that it can be difficult to implement.
- The importance of global cooperation in responding to challenges in cyberspace is emphasized, an example of a successful cooperation between India and the UK in retaining the Wannacry virus is mentioned. The multi-stakeholder approach of the GFCE is key in developing an action plan for cyber capacity building. Government, private companies, intergovernmental organizations, civil society, academia and the technical community will be invited to contribute to the GFCE action plan.

- Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):

- It was suggested to better sync the outputs of various forums, such as the Best Practices Forum of the IGF and the GGP's of the GFCE, to have a complete overview of all cyber capacity building efforts and make sure there is no duplication of efforts. It is noted that information sharing is important, currently the Oxford Portal functions as a tool to map all cyber capacity building efforts.
- The importance of bringing more technical experts and policymakers together was mentioned. While policy and technology mutually impact another, it is valuable to encourage dialogue between government and the technical community. The GFCE can play an important part by connecting GFCE members that have certain challenges with the technical community and providing a platform for cross-stakeholder discussions.
- It is emphasized that international organizations within the GFCE have a wide reach, which should help the coordination among various actors and forums.

Gender Reporting

- Estimate the overall number of the participants present at the session: approximately 50-60 participants were present during the Open Forum.

- Estimate the overall number of women present at the session: approximately 50% of the participants was female.

- To what extent did the session discuss gender equality and/or women's empowerment? The focus of the Open Forum was not on the topic of gender equality and / or women's empowerment.

- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion: not applicable