IGF 2017 Reporting Template

- Session Title:

Cybersecurity 2.0 - Leveraging the Multistakeholder Model to Develop and Deploy Cybersecurity Policy (OF70)

- Date: 20.12.17

- Time: 12:20-13:20

- Session Organizer: Israel National Cyber Directorate, National Telecommunications & Information Administration ,U.S. Department of Commerce

- Moderator: Lea Kaspar, Global Partner Digital's (GPD)

- Rapporteur/Notetaker: Amit Ashkenazi, Legal Advisor, INCD

- List of Speakers and their institutional affiliations:
Amit Ashkenazi, Legal Advisor, National Cyber Directorate, Prime Minister's Office, Israel

Jonah Hill, Policy Expert, Office of International Affairs National Telecommunications & Information Administration ,U.S. Department of Commerce

Dr. Tobias Feakin, Australian Ambassador for Cyber Affairs

Jan Neutze, Director of Cybersecurity Policy, Microsoft

Dr Alison Gillwald, Executive Director: Research ICT Africa; Adjunct Professor: University of Cape Town Graduate School of Development and Policy Practice

- Key Issues raised:

The roles of governments in domestic cybersecurity

The Public-Private interfaces in providing domestic cybersecurity

The role of the "multistakeholder" model in developing cybersecurity policy

The need to tailor and adapt the multistakeholder to domestic contexts

The contribution of the private sector to public policy development

Discussion:

The term cybersecurity for the purposes of the discussion centered around the domestic role of governments in enabling and providing a safe and secure digital ecosystem, to enable innovation and free movement of information. Cybersecurity therefore in the context of the discussion focused on maintaining the safe and proper functioning of computers and networks, and not on the use of such computers and networks on the "content" level.

As cyberspace is composed of organizational networks, the role of the government in providing safety and security is more complex. The discussants raised the value of the multistakeholder model, developed in the general internet governance context in this area. The multistakeholder model is useful to develop the public-private interface needed to protect the proper functioning of the cyber domain. It has utility in importing insights from IT companies that design technological reality, organizations with experience in protecting their networks and the costs of such protection, as well as NGOs, and other stakeholders. This can be translated to a better and more effective cyber policy and its positive deployment. Whether the policy setting is regulatory, such as creating standards, cooperative such as information sharing, or developing a national agenda, insights from multistakeholder discussions promote net positive policies.

It was noted that the multistakeholder approach presumes that the rule of law and the protection of human rights online apply. Therefore its effective application in different domestic settings requires attention to these presumptions and further calibration. In the international context, flushing out common issues and challenges to domestic cybersecurity through domestic multistakeholder discussions can promote global common understandings and ways forward.

Conclusions from the discussion

Drawing from the best practices put forth by the participants and comments from the audience, the panel described the importance of policy development and deployment, based on the actual concerns of the multistakeholder community. The panel highlighted the need for a bottom-up approach, in which domestic stakeholders, lead by a governmental pivotal agency, work together to come up with solutions.

Going forward, this approach could also feed into broader international processes currently taking place. As the international community searches for ways to enhance cybersecurity globally, the input of domestic cybersecurity experts, both governmental and private, emerges as being fundamental to that conversation. The international community, by being receptive to such input, could enable the development of better global interfaces between domestic policies to enhance cybersecurity. Such an approach can constitute a fertile terrain for effective international conversations on cybersecurity to take place.

-**Gender Reporting**

- Estimate the overall number of the participants present at the session:
60
- Estimate the overall number of women present at the session:

30
- To what extent did the session discuss gender equality and/or women's empowerment?
Did not discuss as the issue was not relevant for tha discussion.

- If the session addressed issues related to gender equality and/or women's empowerment,
please provide a brief summary of the discussion: