Proposal for 2017 Best Practice Forum (BPF) on Cybersecurity

As the focus of its efforts in 2017, the Cybersecurity BPF proposes to build on existing work carried out within the IGF. In concrete terms, it would look at the "Policy Options for Enabling and Connecting the Next Billion(s)" (CENB), extract some of these options and gather public comment on how best practices in cybersecurity can support each of them. In 2015, CENB collected and inventorized a set of policy options to enable Internet growth. In 2016, this work continued by looking at regional and local specificities. A very practical set of "things to do" emerges from the document: http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3416/412
Addressing these issues could help the Internet ensure continued progress towards the sustainable development goals.

For a selection of the policy recommendations, BPF members would develop a succinct set of questions to steer the process. Initially the exercise would be to send out for comment a high-level overview of the policies; based on inputs received, the opportunity might arise to delve deeper into some of the issues, particularly ones seen as controversial.

The BPF's main approach to gathering input last year was a highly effective targeted outreach campaign in which experts and organizations were contacted individually by email and their comments solicited – as opposed to broader and more generalized mailing list communication. Such a process would contribute to especially rich inputs this year if it leads to the sharing of local-level best practices from the IGF's National and Regional Initiatives (NRIs), which represent a wide spectrum of stakeholders. Combined with inputs from security teams, civil society, private sector and government participants already active in the BPF, a set of bottom-up cybersecurity recommendations with strong applicability could be developed.

Here is a very practical, rough example of how the CNB document would act as a basis for the process:

The CENB document mentions for SDG 9 ("Industry, innovation and infrastructure") that innovation in technology and the IoT can create opportunities for growth by leapfrogging historic development. However, this is only the case if the growth in these technologies is for instance protected by the ability of organizations to defend themselves from DDoS. If they do not, these economies may still grow, but may be more vulnerable than economies that grew in high bandwidth environments over time. Positive policy learnings from other countries could include e.g. the national DDoS shelter concept operated by KrCERT/CC (a case study in the first year of the CSIRT BPF).

Having these cases documented early could provide a practical tool for developing economies, and would be developed with a multistakeholder starting point and perspective. Given the fact that most cybersecurity recommendations are put forward by governments, providing such a multistakeholder perspective would leverage the strengths and comparative advantages of the IGF community and add value to the global cybersecurity discussions.