IGF 2018 - Proposal for a BPF on Cybersecurity

Culture, Norms and Values in Cybersecurity

I - NAMES OF AT LEAST TWO CO-FACILITATORS (MAG member + non-MAG members as appropriate)

Co-Facilitators: Markus Kummer, Ben Wallis
Lead Expert: Maarten Van Horenbeeck

II - BACKGROUND

In 2016, the first Best Practice Forum on Cybersecurity started off with discussions enabling participants to understand the wider context of the word "cybersecurity" for each stakeholder group. The BPF made it clear right from the beginning that this work needed to be conceived as a multi-year project. It then worked to:

- Identify the communications mechanisms between stakeholder groups to discuss cybersecurity issues;
- Understand the typical roles and responsibilities of each group in making sure the Internet is a secure and safe place;
- Identify common problem areas in cooperation, and good best practices for doing so.

The 2017 BPF explored how cybersecurity influences the ability of ICTs and Internet technologies to support the achievement of the SDGs. Among other things, it

- examined the roles and responsibilities of the different stakeholder groups; and
- aimed to identify options for policy mitigations that could help ensure that the next billion(s) users can be connected in a safe and reliable manner and fully benefit from existing and future technologies.

III - DESCRIPTION:

For 2018, a number of directions were considered for further examination. Two main themes found broad support: the digital divide which develops when some Internet users can afford security, and others cannot; and culture, norms and values of cybersecurity, and how they are important. While it was found that the two themes are interconnected, the proposal for 2018 is to focus on **culture, norms and values in cybersecurity**.

- Norms have become a very important mechanism for states and non-state actors to agree on responsible behaviour in cyberspace. There are numerous initiatives under way in this regard, but with limited exceptions, such as the Global Conference on Cyberspace (GCCS) and the Global Commission on the Stability of Cyberspace (GCSC), most of these norms discussions happen in inter-state forums, and they do not always provide an open and inclusive mechanism for non-state actors to participate and to contribute. In this way, a continuing BPF on Cybersecurity would build on the specificity of the IGF and add value in providing a complementary forum for multistakeholder feedback on this topic.

- The BPF could start the process by building on its previous work on the roles and responsibilities of the IGF stakeholder groups in cyberspace and explore what norms have developed that apply to each of these groups. Some of the questions to be looked into relate to the behaviour of each stakeholder group, such as “state behaviour” or “industry behaviour”. The discussion of civil society’s role in norms development would include social norms of safe and secure online behaviour by individual users.
- Further work will identify norms established by various forums, documenting and comparing them. Of particular value would be the IGF’s network of National and Regional IGF initiatives (NRIs). Through this network, the BPF can bring in a developing country perspective and connect the NRIs with the norms development communities, to promote a culture of cybersecurity. Part of this process would be to make sure that their norms are well known and understood, and to provide a space for discussion.
- This process will result in the development of a document, while the norms development bodies can participate in the BPF for more real-time feedback.
- The BPF can also leverage the work from last year to identify if any of the policy recommendations may see widespread acceptance, and may have developed into a recognized “best practice”. This could then lead to other norms development bodies considering them as new norms - consistent with one of the IGF’s purposes to bring emerging issues to the attention of the relevant bodies.
- Focusing on culture, norms and values will lead us down the path of understanding the impact of a “digital security divide” as well. When or where there’s no real universal implementation of a norm, it may result in a group of “haves” and “have nots” in terms of the protection the norms offer. Security controls will be sufficient or meaningful in some parts of the world, and not in others. This will be an interesting area for investigation into the reasons for non-adherence or potential barriers preventing the implementation.

IV - OUTREACH PLAN AND MULTISTAKEHOLDER ENGAGEMENT IN THE WORK

Multistakeholder engagement and Horizontal areas of focus for 2018

The BPF intends to reach out to all stakeholders and make full use of its existing network of contacts and the mailing list. In addition, this year the BPF plans extra effort to:

- Work proactively to get more governments involved, by collecting best practices which everyone should apply, but which may not be universally known.
- Further engage with the NRIs and get them proactively involved. Perhaps try to find a volunteer in each region to present at their regional events on the topic of norms in cybersecurity, and drive conversation.

Overview of activities of the 2017 BPF on Cybersecurity

BPF Output documents:

- 2017 Best Practice Forum on Cybersecurity outcome document (link)
- Security Policy analysis of CENB Phase I (link)
- Security Policy analysis of CENB Phase II (link)

BPF Activities

- **# of virtual meetings:** 7 (see the BPF webpage for meeting summaries)
- **# of in-person meetings:** 3
    - BPF session at the IGF (see Annex 3 of the BPF output for summary)
    - BPF Cybersecurity coordination and evaluation meeting at the IGF (see Annex 4 of the BPF output for summary)
    - Informal meeting at the GCCS

BPF Cybersecurity mailing list

- **285 email addresses subscribed to the mailing list**
- **Material topics discussed on the mailing list in 2017:**
    - Cybersecurity and fake news
    - SDGs and cybersecurity
    - Responsibilities of different stakeholder groups in cybersecurity
    - Developing cybersecurity culture, norms and values
    - Critical issues in cybersecurity incident response
    - Internet of Things security
    - Security implications of Internet shutdowns

Stakeholder input in the work of the BPF

- The BPF output document is the product of a collaborative effort and was developed in an open and iterative way where stakeholders had multiple opportunities to give feedback on draft versions. Substantive input, however, was collected via an open call for contributions.
- **# of formal submissions:** 27 (the contributions are archived on the IGF website)
    - **Government:** 2
    - **Intergovernmental Organization:** 2
    - **Civil Society:** 19
    - **Technical Community:** 1
    - **Private Sector:** 3
    - **NRIs contributing:** 4

Overview of responses to the BPF's call for contributions
Mr. Shredeep Rayamajhi
Mr. Ben Wallis / **Microsoft**
Dr.N.Sudha Bhuvaneswari
Mr. Foncham Denis Doh / **Cameroon Internet Governance Organization**
Mr. Ji Haojun / **Government of China**
United Nations Cuban Association
Ms. Anita Sohan / **Commonwealth Telecommunications Organisation (CTO)**
Mr. Mohit Saraswat
Mr. Akinremi Peter Taiwo / **African Civil Society on Information Society (ACSIS)**
Mr. Peter Micek / **Access Now**
Mr. Naveen K. Lakshman
Ms. Carina Birarda / **ISOC Cybersecurity SIG**

Ms. Luisa Lobato
Mr. Dave Kissoondoyal / **IGF Mauritius**
Dr. U.M. Mbanaso / **Centre for Cyberspace Studies, Nasarawa State University**
Ms. Amali De Silva-Mitchell
Mr. Opeyemi Onifade / **Africa ICT Alliance (AfICTA)**
Mr. Mohammad Talebi / **Mobile communication Company of Iran (MCI)**
Ms. Lucy Purdon / **Privacy International**
Mr. Koen van den Dool / **Global Commission on the Stability of Cyberspace**
Mr. Alexandru Frunza-Nicolescu / **Cybercrime Division, Council of Europe**
Mr. Sivasubramanian Muthusamy / **Internet Society India, Chennai Chapter**
Ms. Raquel Gatto / **ISOC**
Mr. Nigel Cassimire / **Caribbean IGF**
Mr. Arzak Khan / **Internet Policy Observatory Pakistan**
Ms. Mallory Knodel / **Association for Progressive Communications (APC)**
Ms. Tatiana Tropina / **EuroDIG**

- **Invited expert contributions to the working session in Geneva:**
  - Ms. Cristine Hoepers, **CERT.br**
  - Mr. Benedict Addis, **Shadowserver**
  - Mr. Matthew Shears, **GP Digital**
  - Ms. Deborah Brown, **Association for Progressive Communications**
  - Mr. Alexander Klimburg, **Global Commission on the Stability of Cyberspace**
  - Ms. Kaja Ciglic, **Microsoft**