IGF 2019 - Proposal for a BPF on Cybersecurity

Exploring best practices in relation to recent international cybersecurity initiatives

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 Practices 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 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 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.

The 2018 BPF explored the world of normative behavior in cybersecurity from a multi-stakeholder perspective. It:

- Identified the importance of norms as a mechanism in cybersecurity for state and non-state actors to agree on a responsible way to behave in cyberspace;
- Studied the importance of multi-stakeholderism in ensuring norms get the right attention and receive sufficient implementation effort; and
- Identified norms bodies and norms, and how the consistent implementation of norms is critical to avoiding a digital cybersecurity divide.

III - DESCRIPTION:

The final months of 2018 saw several new initiatives at the international level related to security in cyberspace. In November, the Global Commission on the Stability of Cyberspace (GCSC) released its second package of norms in Singapore, while French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace during the IGF in Paris. In December, the UN General Assembly passed two Resolutions initiating new work on cybersecurity, through both the creation of an Open-Ended Working Group (OEWG) and with a new iteration of the Group of Governmental Experts (GGE).

The BPF on Cybersecurity proposes to work in 2019 on the identification of best practices related to the different elements (e.g. principles, policy approaches) contained within these various initiatives.

The **first phase** of the work would be to identify all relevant initiatives and agreements. The analysis will look for horizontal / overlapping elements (those appearing in more than one initiative) as well as for initiative-specific elements (which only appear in one). This work will be published as a first output and serve as a basis for the second phase of the work.

The **second phase** of the work in 2019 would then be to agree which particular elements the work should focus on, and to then collect and share best practices around the implementation of these elements and any related mechanisms and measures. The BPF's existing participants, stakeholders and knowledge base will enable it to identify these best practices. The BPF could also identify existing forums and networks that are currently addressing, or are well-placed to address, the elements that it has decided to cover, and provide an understanding on how stakeholders can participate in those existing processes. The resulting work would serve as a concrete contribution to be fed into whatever processes have been created to take forward the identified elements in the field of cybersecurity.

We propose to carry out this work in the following ways:

- Encourage **widespread participation from each stakeholder group** through focused invitations at the beginning of the year. This will focus on:
    - Existing BPF participants and their communities and partners;
    - Signatories to the Paris Call and other initiatives (where contact information is available);
- **Promote discussion within our multi-stakeholder community** and encourage debate on how the different elements contained within cybersecurity initiatives tie in with, support, and perhaps deviate from, existing normative behavior that was identified during our 2018 BPF effort. This discussion could be summarized as a research paper to stimulate discussion on the Call;
- The Paris Call recognized a **specific reflection on the applicability of international law to the use of ICTs by governments**. Leveraging the group of legal experts that contributed and joined the BPF in 2018, focusing on cyber norms, we will focus part of our analysis on the implementation in legal frameworks of this principle;
- **Publish a Call for Contributions to collect best practices on the identified elements**, and engage with the NRIs to obtain a wider set of insights around how they have been implemented around the world by governments and other appropriate stakeholders;
- Engage specifically with those parties that engage in the BPF, and are signatories to the different initiatives the BPF decides to cover, in order to **learn about any programs or initiatives put in place to support their commitments, e.g. initiatives by signatories of the Paris Call to implement elements contained within the Call.** We would then document these programs to serve as an example or best practice for others to take into account;
- **Engage with existing organizations that have been in the process of collecting best practices** around the identified elements in order to avoid duplication of work. This would include organizations such as the Global Conference on CyberSpace (GCCS) and the Global Forum on Cyber Expertise (GFCE);
- **Bring our work to the 2019 IGF annual meeting in Berlin** in order to:
    - Discuss progress on implementation of the identified initiatives, including the Paris Call on Trust and Security in Cyberspace
    - Convene a group of multi-stakeholder experts for input and debate;
    - Explore opportunities for closer multi-stakeholder cooperation around achieving the respective objectives outlined in the Call and in other relevant initiatives.

IV - OUTREACH PLAN AND MULTISTAKEHOLDER ENGAGEMENT IN THE WORK

Multistakeholder engagement and Horizontal areas of focus for 2019

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.
- In 2018, we started to engage more closely with the NRIs and get them proactively involved. While we did not receive a significant number of submissions that came directly from the NRIs, we plan to continue this outreach in 2019 and find additional opportunities to share our work with them and enable them to contribute.

Overview of activities of the 2018 BPF on Cybersecurity

BPF Output documents:
- 2018 Best Practice Forum on Cybersecurity outcome document (link)
- Background paper on Cybersecurity Culture, Norms and Values (link)
- Presentation covering the last three years of work in the BPF on Cybersecurity (link)

BPF Activities
- **# of virtual meetings:** 2 (see the BPF webpage for meeting summaries)
- **Introductory meeting to introduce the topic to the NRIs**
- CircleID article "Taking a Multi-Stakeholder Look at Cyber Norms"
- Conference Presentation at Haiti Cybercon on the BPF on Cybersecurity
- BPF session at IGF 2018: video and transcript

BPF Cybersecurity mailing list
- **249 email addresses subscribed to the mailing list**

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:** 16 (the contributions are archived on the IGF website)
    - **Government:** none
    - **Intergovernmental Organization:** none
    - **Civil Society:** 10
    - **Technical Community:** 1
    - **Private Sector:** 5

Overview of responses to the BPF's call for contributions (organizations **in bold**)

Shreedeep Rayamajhi **/ Rayznews**
Andrea Chiappetta / **Aspisec**
Afifa Abbas
Anahiby Becerril
Sudha Bhuvaneswari
Marilson Mapa
Cybersecurity Tech Accord
Cristina Cuomo
Amrita Choudhury / **CCAOI**
Angela McKay / **Microsoft**
Deborah Brown / **Association for Progressive Communications (APC)**
Mallory Knodel, Matthew Shears

Article 19 Eastern Africa
IEEE Internet Initiative
WSIS Coalition (AT&T, Intel, Google, Verisign)
Global Commission on the Stability of Cyberspace (GCSC)

- **Invited expert contributors to the working session at IGF 2018:**
  - Louk Faesen, **Global Commission on the Stability of Cyberspace (Technical Community**
  - Ephraim Percy Kenyanito, **ARTICLE 19 Eastern Africa (Civil Society)**
  - Saleeha Salahuddin, **Facebook / Cybersecurity Tech Accord (Private Sector)**