IGF 2020 - 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.

The 2019 BPF explored Best Practices in relation to recent international cybersecurity initiatives, such as the Paris Call for Trust and Security in Cyberspace, the UNGGE 2015 norms, and many others. It identified best practices related to the implementation, operationalization, and support of different principles, norms, and policy approaches contained in these international agreements/initiatives by individual signatories and stakeholders.

III - DESCRIPTION:

The BPF on Cybersecurity in 2019 worked during eventful times, with new international cybersecurity agreements being launched at a regular pace, and even extensive normative work taking place in private sector and civil society, including through the Contract for the Web, which was launched at the IGF in Berlin. As a result, the work completed in 2019 cannot be called finished and there is extensive work that can be done to identify and review these new agreements using a similar model.

The Open-Ended Working Group will also complete its work in July of 2020, and is expected to report to the UNGA later in the year. In addition, new UN initiatives were voted at the end of the year which will be interesting for the BPF to keep track of.

As a result, the BPF is proposing to continue its analysis work in 2020, along very similar lines to the progress we made in 2019:

The **first phase** of the work would be to continue identifying new agreements, their relative scope, and update our research paper to include this new work. The analysis will continue look for horizontal / overlapping commitments (those appearing in more than one initiative) as well as for initiative-specific commitments (which only appear in one).

The **second phase** of the work in 2020 will consist of:

- Selecting a small set of agreements on which we will perform a Call for Contributions to collect additional best practices on their implementation. We realized that the 2019 work could have been more successful if it was more clearly targeted, and we will therefore select a small number of agreements from within those reviewed in 2020 in order to gain additional input on this targeted sub-set of agreements.
- Identify methods of norms assessment, as implemented by different stakeholder groups. Norms assessment includes mechanisms to determine whether a particular norm is adhered to, or if violations are identified and assessed.
- Evaluate the difference between norms-making between government stakeholders, and norms-making between and / or within other communities, in particular the private sector. We expect to draw on the BPF's 2016 work, in which we identified roles & responsibilities, to determine what norms are most important to be implemented or endorsed by a specific group.

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, Cybersecurity Tech Accord, Charter of Trust, and Contract for the Web.
- **Promote discussion on international commitments within our multi-stakeholder community** and encourage debate on how the different commitments tie in with, support, and perhaps deviate from, existing normative behavior that was identified during our 2019 BPF effort. This discussion could be summarized as a research paper to stimulate discussion on the Call;
- **Publish a Call for Contributions to collect best practices on the identified commitments**, 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;
- **Discuss norms assessment in our calls and mailing list. In particular, we will seek to draw a line to other social science disciplines where norms have been dominant forms of rulemaking**, and identify learnings from them which we can apply in cybersecurity. We will do so by inviting academics from norms-related work in other disciplines to contribute their experience to the BPF.
- 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 the commitments.** 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 commitments in order to avoid duplication of work. This would include organizations such as the Global Commission on the Stability of Cyberspace (GCSC) and the Global Forum on Cyber Expertise (GFCE);
- **Bring our work to the 2020 IGF annual meeting in Poland** in order to:
  - Discuss progress on implementation of the identified initiatives;
  - Convene a group of multi-stakeholder experts for input and debate;
  - Investigate opportunities for closer multi-stakeholder cooperation around achieving its objectives.

IV - OUTREACH PLAN AND MULTISTAKEHOLDER ENGAGEMENT IN THE WORK

The BPF intends to reach out to all stakeholders and make full use of its existing network of contacts and the mailing list. During 2019, we focused on engagement directly with governments to make them aware of the work we did. This resulted in an increase of government submissions, which we intend to continue to promote in 2020.

A particular interest of BPF participants is discussion of norms within the private sector, which are often not as much "policy", but have significant implications for cybersecurity. We intend to leverage the relationships built with several private sector initiatives, such as the Tech Accord, in 2020, to help build a wider bridge and engagement with this community.

Finally, it was raised during the 2019 BPF that Civil Society has played a leading role in norms assessment. Civil Society has always been a key contributor in the BPF on Cybersecurity, since its inception, and we intend to continue to solicit input from this community both through direct appeals and encouragement based on last year's submissions.

V – OVERVIEW OF ACTIVITIES OF THE 2019 BEST PRACTICES FORUM ON CYBERSECURITY

BPF Output documents:

- 2019 Best Practice Forum on Cybersecurity outcome document (link)
- Background paper on Cybersecurity Agreements (link)
- Presentation covering the last four years of work in the BPF on Cybersecurity (link)

BPF Activities

- **# of virtual meetings:** 4 (meeting summaries listed at the bottom of the BPF webpage)
- Contribution to the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security – Informal intersessional consultative meeting (link)
- BPF Cybersecurity Update at the "Bringing it all together" IGF2019 session (link)
- CircleID article on "The Operationalization of Norms and Principles on Cybersecurity" (link)
- CircleID article "IGF Best Practice Forums, an Opportunity to Bring your Experience to the Policy Debate (link)
- LinkedIn post "Turning Cybersecurity Agreements into Action" (link)
- BPF session at IGF 2019: report and video

BPF Cybersecurity mailing list

- **346 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:** 12 (the contributions are archived on the IGF website)
    - **Government:** 3
    - **Intergovernmental Organization:** none
    - **Civil Society:** 5
    - **Technical Community:** 1
    - **Private Sector:** 3

    Written input received from (organizations **in bold**)
    Freedom Online Coalition
    FDFA Switzerland
    Taihe Institute
    DFAT Australia
    Alejandro Pisanty
    Tech Accord
    JPCERT
    Orange
    Dalsie Baniala
    Microsoft
    APC
    GCSC

- **Invited expert contributors to the working session at IGF 2019:**
    - Carina Birarda, *CSIRT Buenos Aires Cybersecurity Center*
    - Sheetal Kumar, *Global Partners Digital*
    - John Hering, *Microsoft*
    - Olaf Kolkman, *Internet Society*
    - Dr. Alexander Klimburg, *Global Commission on the Stability of Cyberspace*
    - Dr. Madeline Carr, *Professor of Global Politics and Cybersecurity, UCL and Director of the Research Institute in Science of Cyber Security*