BPF Cybersecurity 2020 - Meeting 1
19 February 2020
Meeting Recording

1) Introduction

Ben Wallis (BPF co-facilitator) explained that the outline proposal for the BPF in 2020 - Exploring best practices in relation to recent international cybersecurity initiatives - was developed following feedback on the list in December and approved by the Multistakeholder Advisory Group (MAG). The main aim of this first meeting is to discuss how to organize and scope out of the work in 2020.

2) Update and discussion on UN initiatives (OEWG, GGE)

The 2019 work of BPF Cybersecurity was presented to the December 2019 OEWG consultative meeting by the BPF's lead expert, Maarten van Horenbeeck. A broader presentation on both BPF Cybersecurity and the IGF 2019 Messages on Security was presented to the 2nd substantive session of the OEWG in February 2020 by Wai Min Kwok of the UN Department for Economic and Social Affairs (DESA), the UN agency which oversees the IGF and a related Informal Paper was also entered into the record.

A first draft of the OEWG final report is expected early March, with an expectation that it will be made public and open to stakeholder feedback. The IGF is mentioned in the OEWG's initial overview of UN actors and initiatives of interest to OEWG. The final session of the OEWG is in July 2020, although there is support to renew the OEWG's mandate.

Wai Min's report of the meeting included that several OEWG members shared concerns about cyber-attacks, increased militarization, and cybersecurity measures undermining development, had underlined the importance of capacity building, and asked for a global list of capacity-building initiatives and Confidence-Building Measures (CBMs). There were divergent views on the applicability of international cybersecurity rules and different interpretations of norms, including those in the GGE package.

Wai Min made some suggestions for the BPF, which were echoed by some BPF members:

- Do more to engage regional actors (e.g. African Union)
- Reach out to encourage the most active OEWG member countries to participate in the BPF
- Pick up some points made at the OEWG in the BPF's 2020 work plan (e.g. requests for more best practice sharing, roadmaps, CBMs) how can we engage those countries active in GGE and OEWG to raise their awareness of the BPF – can do collectively with IGF secretariat

It was also noted that the joint civil society statement, read out by APC at the OEWG meeting, can be found here.

3) BPF 2020 - Exploring best practices in relation to recent international cybersecurity initiatives

Maarten van Horenbeeck, BPF lead expert, set out a two-part plan for the BPF in 2020.

- Part 1 would be to continue identifying new agreements, adding and assessing any particularly relevant agreements adopted since the analysis for the 2019 report - such as the Contract for the Web and the UN General Assembly's Resolution A/C.3/74/L.11/Rev.1 on Countering the use of

information and communications technologies for criminal purposes - and updating the BPF's 2019 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).

- Part 2 would include two exercises:
    - 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.
    - Understanding and documenting methods of norms assessment, e.g. how to assess whether a norm is being violated. This would mean investigating whether lessons can be learned how norms are made applied in other social science disciplines (e.g. concept of "norms contestation"), and would require engaging with academics working both in cybersecurity and in other fields. Maarten invited BPF members to suggest academics that we could reach out to.

Feedback from members included:

- Important to increase diversity of participation in BPF (especially to realize Part 2), but this is only possible if we actively reach out.

- Focusing too much on mapping exercise risks to duplicate last year's BPF and work being done elsewhere. Suggest to narrow the scope by focusing on agreements that are strictly norms-focused (i.e. set aside legally-binding agreements, such as laws and regulations), and focus on norms agreements that have active bodies behind them to support implementation.

- The IGF pilot project on Implementing Internet Standards for a Safer Internet found that many stakeholders feel that norms deployment should be done through legislation and regulation, but that many stakeholders are also against legislation and regulation in terms of Internet standards, and the BPF could consider this discrepancy

- The BPF could categorise how norm adherence can be analysed. This could be done by taking a few norms and looking at publications by states and non-government actors in which they refer to measures (legally binding and not binding) and best practices that were undertaken to implement / adhere to the norm.

- One member asked whether it is possible to ensure that MAG members take responsibility for raising awareness of the work of the BPF? As the BPF's MAG liaison point, Ben Wallis took note of this question and also explained that the MAG is interested to find ways to better integrate intersessional work (BPFs, DCs) with the IGF 2020 thematic tracks which, for BPF Cybersecurity, will be the Trust track; and that a MAG task force has been set up to review best practices for organising and running BPFs, which will report to the MAG meeting in June 2020.

Next steps – Maarten will review the suggestions and incorporate them into a detailed written proposal for how to organize the work in 2020, which will be circulated to the BPF list for comment.