Proposal for a 2022 Best Practice Forum

1. Title

Best Practices Forum on Cybersecurity

2. Names of at least two Facilitators *(at least one of which is a MAG member).*

Facilitators:
Iombonana Andriamampionona (MAG member)
Markus Kummer

Lead Experts:
Sheetal Kumar, Maarten Van Horenbeeck (Leads)
Mallory Knodel
Pablo Hinojosa

3. Background

The Best Practices Forum on Cybersecurity has been organized since 2016, and has brought together a multistakeholder group of experts and contributors to investigate the topic of cybersecurity.

In 2016, the first Best Practices Forum on Cybersecurity started off with discussions enabling participants to understand the wider context of "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.

In 2020, the BPF Cybersecurity built on this report by identifying new international agreements and initiatives on cybersecurity, and performing a deeper analysis of this set agreements, including looking at whether the agreement includes any of the UN-GGE consensus norms; and whether any additional norms are specifically called out. The narrower set of agreements is focused on those that are specifically normative, rather than having directly enforceable commitments. In addition, the BPF explored what can be learned from norms processes in global governance, in areas completely different than cybersecurity.

The BPF Cybersecurity 2021 on the use of norms to foster trust and security, intends to take a deeper look at the drivers of cyber norms and test these norms concepts against historical Internet events, to better understand how specific norms can be effective at mitigating adverse cybersecurity events.

During 2021, the BPF on Cybersecurity:

- Organized five formal virtual meetings and several smaller working group calls
- Published the research paper "Mapping Analysis of International Cybersecurity Norms Agreements" and associated references, and one background paper "Testing Norms Concepts against Cybersecurity Events"
- Published a statement on the IGF and Cybersecurity to the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security
- Organized a session at the Internet Governance Forum 2021
- Provided an update to the NRI Assembly at EuroDIG
- Published a final report
- Maintained an active mailing list which was used both for discussion of our 2021 work program, and to share general references to cybersecurity activity within and outside of the UN context.

While the BPF is not a place for norms development, in the last three years it has proven to be a viable community for anyone to learn about, and contribute, to the emerging discussion around cyber norms.

4. Description:

The BPF on Cybersecurity continues to work during a time of ongoing normative development in cybersecurity. During our work this year, we determined that this work has been valuable – and that normative work today would have been valuable during historical cybersecurity events.

We believe that further work in this area by the BPF on Cybersecurity can inform and support the discussion, development and assessment taking place in the UN GGE and OEWG exercise and elsewhere. We therefore propose to continue some of our work, while extending it into new domains:

1. To **continue identifying further initiatives**, their relative scope, and update our research paper to include this new work. For 2021, we'd mostly focus on identifying new agreements, and new areas of contestation of cyber norms. We'd update our ongoing repository of these agreements, and learn where areas of disagreement exists between them, rather than focusing on agreement, as we have done in the last two years.

2. During 2021, we identified that the voices of those most affected by cybersecurity events provided nuance that was not typically included in secondary or tertiary source reporting. We'll continue our work to identify key incidents and bringing these voices forward so we can learn where norms

development would have benefited from their input.

3. Another learning for us has been the complex interplay between norms and cybercrime legislation. We will initiate an effort to identify where these efforts support each other, collide, or impact the overall work of mitigating impacts major cybersecurity events. This aligns closely to work currently happening under the auspices of the United Nations Ad Hoc Committee on Cybercrime, which launched on February 28th, 2022.

Building on our work in 2021 to build out a dedicated Engagement and outreach workstream, the BPF will also continue to maintain a focus on expanding the participants in our community.

5. Engagement and outreach plan

This should mention the anticipated engagement from different parts of the multistakeholder community, including the names of organisations which have signalled a desire to participate, and intended outreach to attract further involvement in the work of the BPF. Clearly indicate confirmed commitments.

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;
    - Organizations who have chronicled cybersecurity incidents;
    - Academics who have worked on assessment of cyber norms against real life incidents;
    - Non-state "norm entrepreneurs" whose roles in these processes are considered critical.
    - Civil society groups who can bring in the voices of victims
    - Relevant International organisations, including ICRC
    - Governments active at the UN processes on cyber, including the Ad Hoc Committee on Cybercrime
- 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);
- Focus on understanding the emerging work on cybercrime, and its distinctions from the normative engagement we have tracked so far – in particular from a multi-stakeholder perspective;
- Bring our work to the 2022 IGF annual meeting in Ethiopia in order to:
    - Discuss progress on implementation of the identified initiatives;
    - Convene a group of multi-stakeholder experts for input and debate;
    - Discuss the ideas underpinning normative agreements that have been consistent throughout various iterations of documents, and threats/real life incidents discussed in normative communities

6. Furthering the implementation of the IGF Mandate and UN Secretary-General's Roadmap for Digital Cooperation

The BPF on Cybersecurity has historically worked in a number of ways to increase cooperation and strengthen the ties between the IGF and other fora. Below are a few examples of how this has been implemented:

- In 2017, the BPF had an informal meeting at an event other than the IGF, by bringing together a small group of experts at the Global Conference on Cyberspace, in New Delhi, India.
- In 2018, the BPF presented its work effort at a third party cybersecurity conference, Haiti Cybercon.
- In 2019, the BPF contributed its outcome to the Open Ended Working Group on developments in the field of information and telecommunications in the context of international security.
- From 2018 through 2020, the BPF published several articles on CircleID, a website focused on internet infrastructure.

- In 2021, the BPF built out a specific engagement workstream, which led to active sharing of our work and output in other forums, and in particular a presentation to the NRI Assembly at EuroDIG.

Over the years, the BPF has gradually grown its amount of volunteers and contributors, and we are an active community that stretches well into each of the stakeholder groups represented at the IGF. As an outcome of our 2021 work, the BPF has already proposed a follow-up session at the annual Rightscon conference, and we will continue to work on these types of opportunities in the proposed 2022 iteration of the group.