Proposal for a 2021 Best Practice Forum

1. Title

Best Practices Forum on Cybersecurity on the use of norms to foster trust and security

1a. Executive Summary

The 2021 BPF Cybersecurity proposal looks to build upon, and leverage the strengths of, the 2020 Cybersecurity BPF in ways that will support the ongoing development of cybersecurity norms in the UN and elsewhere. While continuing to identify relevant cybersecurity norms agreements, the BPF will develop the work by looking more deeply into both the drivers behind, and disablers of, cyber norms. Secondly, by reviewing major historical cybersecurity incidents, we hope to understand how they can help drive further norms discussions. For example, we will evaluate whether existing norms would have been successful at mitigating previous adverse events, and also look at how security events might have supported implementation and / or expansion of norms. A new dimension to this year's work will be to bring in the voice of victims of cybersecurity incidents and those who of responders to incidents. Finally, we also hope to broaden our thinking about how to strengthen norms in cybersecurity by looking into examples of dealing with incidents in other areas, such as environmental protection.

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

Facilitators:
Iombonana Andriamampionona (MAG member)
Markus Kummer

Lead Expert: Maarten Van Horenbeeck

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 of agreements, including looking at whether the agreements include any of the UN-GGE consensus norms; and whether any additional norms are specifically called out. The narrower set of agreements was 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.

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

During 2020, the BPF on Cybersecurity:

- Organized three formal virtual meetings and several smaller working group calls
- Published one research paper, "Exploring Best Practices in Relation to International Cybersecurity Agreements" and one background paper "What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance"
- 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
- Issued a Call for Contributions, which resulted in five formal submissions
- Organized a session at the Internet Governance Forum 2020.
- Published a final report
- Maintained an active mailing list which was used both for discussion of our 2020 work program, and to share general references to cybersecurity activity within and outside of the UN context.

4. Description:

As was the case in 2019, the BPF on Cybersecurity worked during a time of ongoing normative development in cybersecurity, including during one iteration of the UN Government Group of Experts and the Open Ended Working Group focused on the topic of cybersecurity. Significant implementation efforts are underway to widen the impact of cyber norms development, across all stakeholder communities. In particular, we are seeing emerging evidence of norms assessment and contestation taking place.

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 exercises and elsewhere and we therefore propose to continue along three work streams, similar to last year:

1. To **continue identifying further 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).

   Whereas in 2019, we focused on overlapping commitments (those appearing in more than one initiative), and in 2020, we took a wider look at initiative-specific commitments (which appear in only one); during 2021, we intend to take a deeper look at the drivers of cyber norms. These may include concerns raised by internet users, security incidents, and other events. We plan to take a closer look at which ideas behind the norms have shown continuity during various incidents and stages of problematic behavior.

2. To identify criteria to select major historical cybersecurity events (including adverse events such as incidents) that have informed cyber norms development.

3. We will review those events that match these criteria**, and evaluate how they can further help drive specific norms discussion.** We'll evaluate whether existing norms would, if implemented, have been successful at mitigating any adverse events. We'll also review how security events may have supported norms implementation, or expansion of the scope of an existing norm.

4. We plan to bring in the voice of victims of these incidents, and the responders, to evaluate which norms would have been able to reduce the impact of these security incidents, and how. We will also expand our inquiry into examples from other fields, for example environmental protection.

5. Based on this analysis, we **will review which core ideas behind the normative agreements had the most continuity through various incidents** and which themes have additional potential in the dialogue. We'll aim to identify in how actors engaged with these ideas, such as how they communicated, and how resources were mobilized and norms discussion promoted that helped drive new norms development.

The BPF will also continue to maintain a focus on expanding the participants in our community, this year specifically focusing on incident responders, organizations working with victims of cybersecurity incidents, and academics focused on the practical roots and applications of cyber norms.

In addition to continuing to build on, and leverage the strengths of last year's work, this additional approach, focused on incidents and victims, will help explore a new dimension of cyber norms work, and help inform these efforts across our multi-stakeholder 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.
- Publish a **Call for Contributions to collect the experiences of those affected by security incidents**, and to what degree those experiences may have resulted in normative behavior in various normative communities.

- Engage specifically with those parties that participate 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.
- 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;
    - 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 will consider increasing its commitment through the following initiatives:

- Share its learnings and progress at conferences and other thematic events outside of the IGF
- Cooperate with other actors and groups invested in the same area and interests
- Leverage the increased virtual nature of collaboration within the IGF to increase participation from experts in LDCs and SIDS

In addition, the BPF on Cybersecurity, by creating a space for voices affected by major security incidents, and evaluating which normative activity would likely be successful at preventing such behaviors, would support the UN Secretary-General's call for a statement by all UN Member States on Digital Trust and Security set out in his Roadmap for Digital Cooperation.