Call for Contributions of the 2019 BPF on Cybersecurity
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.

2019-09-09, Paris, France

1. *Is your organization a signatory to any of the agreements covered, or any other ones which intend to improve cybersecurity and which our group should look at? If not, we are still interested in your opinion on the rest of this questionnaire!*

   Orange Group is involved in the Mutually Agreed Norms for Routing Security (MANRS) as well as other initiatives such as Paris Call. Moreover, Orange is member of several standardisation bodies such as the GSMA or the 3GPP, etc. which also aim at increasing cybersecurity in past and future norms or protocols.

2. *What projects and programs have you implemented or have seen implemented to support the goals of any agreements you signed up to? Do you have any plans to implement specific projects?*

   Orange Group is working on integrating each of its affiliates – both Europe and AMEA, inside the MANRS initiative. Orange Group launched a program in order to encourage and accompany affiliates to enhancing the level of security of their networks (e.g., IP routing security policy, IP anti-spoofing policy). Currently, three Orange Group’s affiliates are involved inside the MANRS initiative and six other affiliates are working to be compliant with the MANRS initiative requirements.

3. *During our review, we identified a few key elements that were part of multiple agreements and seem to have more widespread support and/or implementation. Do you have views around the relative importance of these (e.g. by providing a ranked list), or are there any others that you consider to be significant commitments in these types of agreements?*

- ***Furthers multi-stakeholderism:** identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.*
- ***Vulnerability equities processes:** the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.*
- ***Responsible disclosure:** the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.*
- ***Reference to International Law:** whether the agreement reflects on the importance of aligning international law.*
- ***Definition of Cyber threats:** whether the agreement proposes a clear or aligned definition of cyber threats.*
- ***Definition of Cyber-attacks:** whether the agreement proposes a clear or aligned definition of cyber attacks.*
- ***Reference to Capacity Building:** whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.*
- ***Specified CBM's:** whether the agreement describes or recommends specific Confidence Building Measures.*
- ***Reference to Human Rights:** whether the agreement reflects on the importance of human rights online.*
- ***References to content restrictions:** whether the agreement discusses the need for content restrictions online.*

Regarding MANRS initiative, Orange's significant commitments are:

- Further multi-stakeholderism
- Responsible disclosure
- Definition of Cyber threats
- Reference to Capacity Building

4. *What has the outcome been of these agreements? Do you see value in these agreements either as a participant, or as an outsider who has observed them?*

Digital technologies and the Internet are the backbone of our society and economy. They are deeply changing our lifestyles and organizations.. This is why, at Orange, as trusted connectivity provider we are always looking for greater reliability and security. The adherence to MANRS initiative is part of our commitment to cooperate with leading actors, like ISOC, in order to improve the security for all through preventing routing disruptions.

5. *Have you seen any specific challenges when it comes to implementing the agreement?*

   Because enforcing a strong routing policy might increase the number of false positives and rejects, this part has to be studied by operational teams in order to ensure that customer will not be negatively impacted. This might or might not, introduce a slight delay in hardened routing policies being activated in production.

6. *Have you observed adverse effects, or tensions from any of the elements of these agreements, where specifics may be at odds with intended end results? For instance a commitment that may seem like it improves cybersecurity at first sight or tries to fix one issue, but has effects that lead to a reduction in cybersecurity?*

   Orange did not observe adverse effects after implementing the MANRS agreement recommendations.