Call for Contributions on the 2019 BPF on Cybersecurity

The IGF Best Practices Forum on Cybersecurity is a multistakeholder group focusing on identifying best practices in Cybersecurity. From 2016-2018, the group has focused on identifying roles and responsibilities of individual stakeholder groups in cybersecurity, and investigated the development of culture, norms and values in cybersecurity.

In 2019, the BPF Cybersecurity is focusing on international agreements and initiatives on cybersecurity. The main objective of this year's effort is to identify 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. initiatives. Amongst others, these agreements include for instance the Paris Call for Trust and Cybersecurity in Cyberspace, the Tech Accord, the Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security and the 2015 UNGGE proposed norms.

The IGF Best Practices Forum on Cybersecurity is calling for input for its 2019 effort. We are soliciting input by Friday 20 September 2019.

For a better understanding of the types of agreements we are investigating, we recommend reading the background paper published by the BPF Cybersecurity. and available here (.pdf) . The paper provides an overview of international agreements and initiatives by focusing on the (i) identification of spaces for agreement, (ii) assessment of the state of existing agreements and (iii) next steps for implementation.

Please find below the list of questions. We recommend that, when *possible* and *applicable*, contributors refer to the list of initiatives outlined in Annex A.

Instructions.

Please attach contributions as Word Documents (or other applicable non-PDF text) in an e-mail and send them to bpf-cybersecurity-contribution@intgovforum.org . You're kindly requested to try to keep the contributions to **no more than 2-3 pages**, and to include URLs/Links to relevant information.

Contributions will be published on the BPF webpage and included in the BPF's output document. Please inform us here, should there be any limitations on the publication of your contribution, and indicate what title, organisation or contact person could be used to identify your contribution.

We are soliciting input by **20 September 2019**.

Questions

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!- No

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? - Through the programs that I have been leading in 2018 – through the Regulator's Office, I have initiated what we called **"Community Consumer Champions"**. We used these champions across Vanuatu and provide basic training to them. Then, the Regulator's office then, use them on other consumer Protection

activities including basic awareness on cyber-security and why it is important for users of internet and other digital devices to be safe and secured while surfing online.

Away from the Regulator's Office, this year, I have done a lot with Youth Development through **Faith Based Organisations**. Through the church that I am attending, as one of the activities for the Church, I focused on developing youths by planning a weekly program for them. I have been taking youths through **debates** of real life including issues related to cybersecurity, social media and more other online activities. I also used sports given Youths are very much interested in sports, so I used **sports** especially volleyball, Rugby and soccer even hiking, to get them together and take the opportunity to hear from them views on ICT development including cyber security awareness. During that time, I bring institutions like the Regulator's office to give them more information on cyber-safety and Security. **Camping** is another activity that most youths cannot missed. So I bring them to one youth camp (have them all together), then, prepare program for them to be part of, and one of which is hearing information about cyber-security and safety, what is expected and a little bit of information on other ICT development including artificial intelligence.

However, because all of these are voluntarily base activities that I initiated to keep the youth together, away from mischiefs and bad behaviors, I used my own funds to coordinate and facilitate these activities which the youth are very much enjoying themselves and learning more. Sometimes, I request for tiny contributions from church if they have any left over to support such important activities.

The Company that we have established called **"Pacific Inspiro Limited"** (a service consulting firm focusing on inspiring vulnerable groups and other targeted customers on many services of which they needed assistance on) has just formally born this year and we are still building its roots financially, thus, I have to invest a lot of my time and efforts doing something of my passion in the rural communities at my own cost but under the name of this firm.

However, through the Vanuatu Internet Governance secretariat http://www.internet.org.vu/, there is also a lot of awareness through schools and university of the South Pacific (campus) based in Port Vila. I am sure we can learn more from their programs which they have outlined for the coming months.

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.

In my view, we should consider situational cases but at the national level. For example, for small island states (pacific region) our agreements can be done but consider applying bottom up approach which will be much more effective given most of these activities are stirred up by those who have no hope to source assistance in an acceptable way. Consider agreements or arrangements, to me, if we want to see effectiveness of these arrangements, then we start of by initiating at the much lower level. At the same time, come up with incentives that will bring attention and support from that said level. For example, based on the above highlighted, initiate an agreement with the effective organisations with the government back up and support towards these identified organisations, and some conditions in those agreements is to invest on key activities for cyber security but focus more on the rural communities who don't have much access to same opportunities as those who live in town or cities. Additionally, agreements also include the Service Providers meeting the requirements etc……. agreements that will include their investment on how best would at the national level would the each responsible organisation and service providers support particularly on finding a practical solution which I am sure, there is to assist keep the users from being hacked.

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? – I do see value of those agreements only if we consider a bottom up approach and have the international (UN agencies) level and the National Government recognition. The agreement with the National Government and the UN agency is to annually support these identified organisations who have signed the agreement and these organisations to be recognized or incentivized on what they are doing or being doing given these activities are side activities and not so much of a top priority of the selected organisation.

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

   The only Challenge is the enforcement and back up support from the high level. If there are compliance agency/or service organisations whose jobs is making sure they enforce these agreements, these identified orgnisations will deliver. Majority of the Government organisations (in the Pacific region) do not really understand their legislative obligations or even have time to read what they are bind to deliver on.

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? -

   In my view the adverse effects that I can see now is related to costs. If this can be resolved or there are ways how to handle this then, I think it is going to initially work out positively. However, if there are hard core and very technical equipment be involved in this process then, that is another thing that we should be prepared for as to how to handle this given the limited capacity across the world on using high powered or clever machines that only 0.1% knows how to handle it.

Annex A: List of agreements for consideration

- The G20, in their Antalya Summit Leaders' Communiqué, noted that "affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors".
- The G7, in their Charlevoix commitment on defending Democracy from foreign threats, committed to "Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state."
- The Cybersecurity Tech Accord is a set of commitments promoting a safer online world through collaboration among technology companies.
- The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security frames cyber security approaches in a human rights context, and originates from a set of member governments.
- In the Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security member states of the Shanghai Cooperation Organization agree on major threats to, and major areas of cooperation in cybersecurity.
- The African Union Convention on Cyber Security and Personal Data Protection assists in harmonizing cybersecurity legislation across member states of the African Union.
- The Council to Secure the Digital Economy is a group of corporations which together published an International Anti-Botnet guide with recommendations on how to best prevent and mitigate the factors that lead to widespread botnet infections.
- The League of Arab States published a Convention on Combating Information Technology Offences which intends to strengthen cooperation between the Arab States on technology-related offenses.
- Perhaps one of the oldest documents, the Council of Europe developed and published a Convention on Cybercrime, also known as the Budapest Convention. Adopted in November 2001, it is still the primary international treaty harmonizing national laws on cybercrime.
- The East African Community (EAC) published its Draft EAC Framework for Cyberlaws in 2008, which contains a set of recommendations to its member states on how to reform national laws to facilitate electronic commerce and deter conduct that deteriorates cybersecurity.
- The Economic Community of Central African States (ECCAS) in 2016 adopted the Declaration of Brazzaville, which aims to harmonize national policies and regulations in the Central African subregion.
- The Economic Community of West African States (ECOWAS) Directive C/DIR. 1/08/11 on Fighting Cyber Crime within ECOWAS, agree with central definitions of offenses and rules of procedure for cybercrime investigations.
- The European Union in 2016 adopted, and in 2018 enabled its Directive on Security of Network and Information Systems (NIS Directive). The Directive provides legal

measures to improve cybersecurity across the EU by ensuring states are equipped with incident response and network information systems authorities, ensuring cross-border cooperation within the EU, and implement a culture of cybersecurity across vital industries.

- In December of 2018, the EU reached political agreement on a EU Cybersecurity Act, which reinforces the mandate of the EU Agency for Cybersecurity (ENISA) to better support member states. It also built in a basis for the agency to develop a new cybersecurity certification framework. In May 2019, the EU adopted and authorized the use of sanctions in response to unwanted cyber-behavior.
- The NATO Cyber Defence Pledge, launched during NATO's 2016 Warsaw summit, initiated cyberspace as a fourth operational domain within NATO, and emphasizes cooperation through multinational projects.
- In 2017, the EU Council published to all delegations its conclusions on the Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. This reinforced several existing EU mechanisms, such as the EU Cyber Security Strategy, and further recognized other instruments such as the Budapest Convention, while calling on all Member States to cooperate on cybersecurity through a number of specific proposals.
- The Mutually Agreed Norms for Routing Security (MANRS), an initiative by the Internet Society, is a voluntary set of technical good common practices to improve routing security compiled primarily by members of the network operators community.
- The Southern African Development Community Model Laws on Cybercrime were developed with the intent of harmonizing ICT policies in sub-saharan Africa.
- The Paris Call for Trust and Security in Cyberspace**,** launched by France at the 2018 IGF, currently has 547 official supporters, including 65 states.
- UNGGE Consensus Report of 2015
- The Siemens Charter of Trust contains several product development norms, such as "user-centricity" and "security by default"
- GCSC Six Critical Norms **-** At the time of writing, the six critical norms are still in draft, and published for public input.