**Submission by Dr. Fitriani Bintang Timur, Centre for Strategic and International Studies (CSIS) Indonesia to the informal intersessional consultative meeting of the Open-ended Working Group (2-4 December 2019)**

*Firstly*, it needs to be recognised while Confidence Building Measures can be considered universal, but in the multi-stakeholder engagement, each stakeholder may have different perceptions, languages and understanding depending on their roles, experience, political, economic, cultural and social context that need to be bridged, and that bridge is **education** as capacity building.

*Secondly*, is also important to bridge understanding in the regional, national and local level. It is important to have a common document with a list of definitions and/or terms that stakeholders can refer to. The publication of "Definitions of cyber terms" by Cybersecurity Tech Accord mentioned yesterday is a good example. That said, it is also important to have the **localisation of language** for outcome documents, and/or cyber norms, to enable awareness, understanding and implementation at the national and local levels.

*Lastly*, all stakeholders should partner in addressing the pertinent issue of the human dimension of cyber security through providing education on digital literacy. Specific capacity building interventions should be given to vulnerable populations to provide access and empowerment in the cyber space. I support Canada and Luftbrücke delegates' call for a **targeted capacity building program, that of gender in cyber security and women in cyber security, synergising such effort with the Women, Peace and Security agenda that has already been adopted by many states and regions**.

In Indonesia we have a specific program for cyber security awareness for women, through the framework of Women in Tech, and Women for Peace in the intervention of counter-terrorism. In Southeast Asia, ASEAN has adopted a Joint Statement on Promoting Women, Peace and Security.

Moreover, we need to remember other vulnerable populations, such as minorities, indigenous people, as well as lower economic societies, in their access of cyber space, to ensure their access to a stable and secure internet. Admittedly, the challenge lies in the sustainability of the interventions, because often, approaches to intervention are **project based** and therefore, there is a need to create local ownership in capacity building efforts to make any effort of cyber security capacity building sustainable.

**Way Forward on Multi-stakeholder Approach**

It needs to be recognized that security and stability in cyberspace cannot be achieved solely by member states alone, therefore a multi-stakeholder approach should be a fundamental part of the global cooperation for the pursuit of cybersecurity. There is much to be gained and learned from different stakeholders' engagement in various issues of ICT threats, also on their efforts to address these challenges.

Although there is a differing level of engagement and formalities in multi-stakeholder approaches, arguably such dialogue is an enriching and meaningful way to gather varieties of concerns and vocabularies in formulating future pathways for ICT norms. Multi-stakeholder

would translate to better buy-in to reach critical commitment on the common safety and stability standards of the internet.

Hence, it is considered important to establish a regular multi-stakeholder dialogue to provide feedback and input to a forum such as this. Such an effort can be achieved through four approaches:

1. Agenda – There is a need to have an agenda that would list down all the multi-stakeholder dialogues that would detail the open channel for consultation, where various actors including civil society groups could apply for participation and that efforts should be made to include their concerns in the agenda.

2. Alignment – Prior to having dialogue, there is a necessity to have the stakeholders aligned by identifying the stakeholders and make sure that the meeting is attended by as diverse as possible, if not all voices are being represented. Efforts need to be done to include especially vulnerable groups in the dialogue, through sponsorship for attending. The meeting should also include technical experts and policymakers that could weigh-in on the implement-ability of the outcome document

3. Coordination and collaboration – The ICT development in international security multi-stakeholders dialogue should be coordinated and collaborated with other existing dialogues on technology and the internet. For example, ensuring the sustainable engagement of civil society, academia and industry in the Open-ended Working Group intersessional consultative meeting to have synergy with the OEWG outcome and also provide input for the UNGGE mechanism.

Multi-stakeholder dialogue should be encouraged to be undertaken at the regional and national levels.

4. Platform of registry. There is a need to have a platform of registry to place all summary of outcomes on meetings on the developments in the field of information and telecommunications in the context of international security, including existing cyber norms, cybersecurity reports from different regions, as well as best Practices done by Best Practice Forum Cybersecurity of the Internet Governance Forum. Such a registry platform of cybersecurity dialogue outcomes should be available for the public so cross-reference can be done. This platform would be beneficial to avoid duplication of efforts, while reviewing and updating meeting outcomes should also be done to ensure the relevance of certain norms and agreements.