Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG).

April 2020

Ecuador wishes to commend the efforts made by the President of the Open-Ended Working Group and welcomes the initial pre-draft as an excellent basis for further discussions during this historic first inclusive process, and in addition to the Remarks to the initial pre-draft and positions contained in NAM Working Paper for the Second Substantive Session Ecuador wishes to make the following remarks in its national capacity:

A. Introduction

The OEWG should also consider the differentiated impact that the misuse of ICTs could have for developing countries, as well as the differentiated impact that the misuse of ICTs could have over different demographic groups, including those in a situation of particular vulnerability.

Ecuador believes that gender-related data is instrumental in driving evidence-based policymaking, informing capacity building, and to address the gender impacts of cybersecurity policies and capacity building in technical, policymaking and diplomatic spheres. Also, the OEWG should acknowledge the importance of women's participation in policymaking and negotiations.

B. Existing and Potential Threats

Digital space should be preserved from militarization, and the increasing automation and autonomy in ICT operations is indeed a specific concern. Both elements are appropriately reflected in this section. However, the concerns about the possible disruption of technical infrastructure essential to political processes such as elections, referenda or plebiscites should also be more widely reflected.

It is also central to note and to include in the draft that cyber threats, policies, initiatives and operations can have gender-differentiated impacts. Furthermore, when mentioning the impact on vulnerable populations and particular groups the Pre-draft should include persons with disabilities.

The pre-draft shouldn't only refer to different levels of ICT security and resilience but also to different levels of development.

C. International Law

Ecuador believes this section accurately and carefully reflects the discussions since the beginning of the OEWG. In that regard Ecuador is supportive of the initial pre-draft approach to the different elements on international law.

Furthermore, Ecuador recognises the importance to uphold women's and children rights online, in the context of recognising the applicability of international human rights law, because of the differential threats they experience due to cyber incidents.

We insist on the importance of women equal participation and full involvement in all efforts for the maintenance and promotion of peace and security, including in the cyberspace. During the deliberations Ecuador acknowledged the centrality of the Security Council resolution 1325 on women and peace and security.

D. Rules, Norms and Principles for Responsible State Behaviour

Ecuador emphasises on the need for a wider recognition of asymmetries in the capacity to implement norms, rules and principles of responsible behaviour of States; as well as the differentiated effects that an ICT incident, for example, would have on a specific critical infrastructure in a developing country. Ecuador supports the sharing and dissemination of good practices and lessons on norm implementation, as this could serve to identify needs for cooperation but also possible gaps in order to propose eventual additional norms.

With resolution 73/27 the UN General Assembly decided to convene the OEWG to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour. Ecuador therefore believes that the draft in addition to the development of new norms could also include guidance elements on how to operationalize the existing ones. In that regard Ecuador suggests, for example, the following **guidance** on norm 13.b (GGE 2015)[1]**:**

> i) *States could establish the national structures, policies, processes and coordination mechanisms necessary to facilitate careful consideration of severe ICT incidents and to determine appropriate responses; ii) then States could develop ICT incident assessment or severity templates to evaluate and assess ICT incidents; iii) transparency about and harmonisation of such templates by regional organisations could ensure commonality in how States consider ICT incidents and improve communication between States; iv) when considering all relevant information in the case of an ICT incident, States should conduct research on possible gendered impacts, and work inclusively with all stakeholders to understand the broader context of an ICT incident, including its impact on the enjoyment of women's rights.*

Similarly, the following guidance is proposed for the implementation of norm 13.c[2]:

> *i) if a State identifies malicious cyber activity emanating from another State's region or cyberinfrastructure, a first step could be notifying that State. Computer Emergency Response Teams (CERTs) are crucial to being able to identify such activity; ii) given that ICT incidents can emanate from or involve third States, it is understood that notifying a State does not imply responsibility of that State for the incident; iii) the notified State should acknowledge receipt of the request via the relevant national point of contact; iv) when a State has knowledge that its territory or cyberinfrastructure is being used for an internationally wrongful act that is likely to produce serious adverse consequences in another State, the former State should endeavour to take reasonable, available and practicable measures within its territory and capabilities, consistent with its domestic and international law obligations, to cause the internationally wrongful act to cease, or to mitigate its consequences; v) this norm should not be interpreted as requiring a state to monitor proactively all ICTs within its territory, or to take other preventive steps; vi) a State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond may choose to seek assistance from other States, including through standard assistance request templates; vii) in such cases, assistance may be sought from other States, or from a private entity, in a manner consistent with national law. Commitment by states to cooperate with other nations and assist them in the event of a crisis is instrumental, particular emphasis should be made on the differentiated impact that an ICT incident on a specific Infrastructure could have in a developing country.*

[1] in case of ICT incidents, States should consider all relevant information, including the broader context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences

[2] States should not knowingly allow their territory to be used for internationally wrongful act using ICT´s

The draft should also include new norms; among others the following: *"States should not conduct ICT operations intended to disrupt the technical infrastructure essential to political processes, such as elections, referenda or plebiscites."*

E. Confidence-building Measures

In this section, the draft should reflect the importance to encourage the tailoring and conduct of exercises to test or practice complex and realistic scenarios that may impact their ecosystem, taking into consideration the participation of multiple State holders, including CERTs, CSIRTs, policymakers, diplomats, and other relevant actors.

Also, it is key to prioritise the establishment of a list of a national contact point at the senior diplomatic level to facilitate work for cooperation and international dialogues on cybersecurity and cyberspace. Ciberdiplomacy plays an instrumental role on building confidence among States, therefore cybersecurity and cyberspace issues should be incorporated in training courses and training for diplomats and officials of the Ministries of Foreign Affairs and other government agencies.

F. Capacity-building

There is a need for a comprehensive and progressive vision on the subject, which should necessarily include a gender approach and a sustainable development dimension in all capacity-building strategies.

Ecuador insists on the need for the recognition of asymmetries in the capacity to implement norms, rules and principles of responsible behaviour of the States.

With regard to paragraph 56, when implementing cyber security strategies and when delivering cyber capacity building, States should consider: i) integrating their obligations to protect, promote and uphold women's human rights as part of their cybersecurity strategies; ii) utilising Women Peace and Security National Action Plans in line with the Security Council adopted resolution No 1325, or opportunities provided by other frameworks to advance women's participation within international cybersecurity, alongside their protection; iii) conducting gender reviews of national or regional cybersecurity policies to identify areas for improvement; iv) maintaining sex- or gender-disaggregated participation records for all cybersecurity-related work (diplomacy, capacity building, incident response, etc.); and recognising that capacity-building must be gender-sensitive and gender diverse.

G. Regular Institutional Dialogue

Ecuador appreciates the way the Chair structured this section. In addition to the recommendations contained in the NAM working Paper that could improve the draft, Ecuador wishes to stress the importance of establishing a list available to all Members of a national contact point at the senior diplomatic level to facilitate work for cooperation and international dialogues on cybersecurity and cyberspace.

❖