Introduction

2. …

…In this regard, the OEWG acknowledged the importance of addressing its mandate in a balanced manner and the need to give due attention to both further develop common understandings between States on the use of ICTs, as well as to further the implementation of existing commitments.

3. The OEWG is committed to engaging stakeholders in a systematic, sustained and substantive manner, in accordance with the modalities agreed by silence procedure on 22 April 2022 and formally adopted at the first meeting of the third session of the OEWG on 25 July 2022, and in line with its mandate contained in General Assembly Resolution 75/240 to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia. While different views were expressed on the preferred modalities to be adopted, the eventual agreement was a positive step that demonstrated flexibility on the part of all delegations. The OEWG recalled the importance of engaging other actors, including the private sector, civil society, academia and the technical community, where appropriate, in State’s efforts to implement the recommendations of previous OEWG and GGE reports [2021 OEWG report para 3].

4. The OEWG recognized that regional and sub-regional organizations have made significant efforts in the field of security in the use of ICTs and recalled the important role of regional and sub-regional bodies in taking forward the assessments and recommendations of previous GGE [and OEWG] reports. In addition, regional, cross-regional and inter-organizational exchanges can establish new avenues for collaboration, cooperation, and mutual learning. As not all States are members of a regional organization and not all regional organizations focus on the issue of security in the use of ICTs, the OEWG noted that regional efforts are complementary to the work of the UN and other organizations on this issue.

5. …

…and of promoting the effective, full, equal, and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security.

Threats

[new text proposal for para 7(a) forthcoming]

7(b) Bearing in mind the interrelated and mutually reinforcing nature of the pillars of the OEWG’s mandate, States proposed technical and cooperative measures to address existing and potential threats with regard to security in the use of ICTs through appropriate fora, including:

(i) Cooperation and assistance to establish and strengthen Computer Emergency Response Teams (CERTs). [Move (i) to Capacity building chapter (as per para 61 of 2021 OEWG; para 89(b) of 2021 GGE; para 20(a) of 2015 GGE report)]

(ii) Developing and disseminating comprehensive best practices on the classification and protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII) and the voluntary provision by States of their national views of categories of infrastructure they consider critical and national efforts to protect them [GGE 2015 16(d)]; OR the voluntarily sharing of national views on the classification of critical national infrastructure and critical infrastructure providing essential services regionally and internationally [OEWG 2021] [Move (ii) to confidence]
building chapter (as per 2021 GGe para 85; 2015 GGE report para 16(d)) or norms chapter (rewording of norm 13(g));

(iii) Cooperation and assistance to ensure the integrity of the supply chain, and prevent the use of harmful hidden functions; [Move (iii) to norms chapter - it is a paraphrasing of norm 13(i)]

(iv) Sharing of risk assessments and technical information between States including relevant threat intelligence assessments and compendiums; [Move (iv) to CBMs chapter (as per transparency measures set out in OEWG 2021 para 50; GGE 2021 para 82 and 83;)]

(v) Cooperation and assistance for developing ICT security baseline studies and designing security as a critical requirement; [Move (v) to capacity building chapter, given ref to cooperation and assistance]

(vi) Undertaking international exercises and technical training including of law enforcement officials in coordination with other relevant processes and entities [Move (vi) - corresponds to norm d) ‘assist each other, prosecute terrorist and criminal use of ICT’].

(vii) Prioritizing mutual legal assistance in coordination with other relevant processes and entities;

(viii) Enhancing tailored capacity building efforts; [Move (viii) to capacity building chapter; ‘tailored’ is a reference from 2021 OEWG Capacity building principles]

(ix) Measures and initiatives to strengthen data security; [Move (ix) regarding measures to enhance data security - could be addressed under norm (a)]

(x) Measures to safeguard the general availability and integrity of the internet. [Move (x) to norms chapter - corresponds to norm (f)]

Norms

8.

(a) States consider developing additional guidance or checklists on norms implementation, elaborating and building upon the conclusions and recommendations agreed to in previous OEWG and GGE reports, as well as consider developing common understandings on technical ICT terms.

(c) Information exchange on best practices and cooperation could be enhanced, potentially drawing from models of information sharing in other fields, and could include topics related to norms (g) and (i) – such as innovation, vulnerability disclosure, the protection of critical infrastructure and cooperation between CERTs.

Recommendations:

2. Interested States or groups of States are invited to submit working papers to contribute to the development of States continue exchanging views at the OEWG with the aim of developing guidance and checklists and common understandings on technical ICT terms along with other tools to assist States in developing common understandings on as well as facilitating the implementation of rules, norms and principles of responsible State behaviour in the use of ICTs. Such working papers could facilitate a focused exchange of views at the OEWG.