Open Ended Working Group in the Field of Information and Telecommunications in the Context of International Security

Introduction and Existing and Potential Threats

Comments and Textual Proposals

NEW YORK, 25 July 2022
A. Introduction

Paragraph 1

Comments

- [para 1, 1st sentence] We strongly value the reference to the challenging geopolitical environment. We would like to emphasize the impacts of malicious ICT activities, particularly on critical infrastructure and essential services. The latter are important elements of our work. So at the end of the sentence, after “with rising concern over the malicious use of ICTs by State and non-state actors” we would like to add: against critical infrastructure and essential services, including in the context of armed conflict.

- [para 1, 2nd sentence] We would like to propose an edit that would include a reference to the work of the GGE. We believe it is important to highlight the work of both processes, in line with resolution 76/19 that endorsed the two consensus reports.

- [Para 1, final sentence] We welcome the additional reference in this sentence to the consolidation of an initial framework that the OEWG builds upon. We would like to propose a minor edit to underline the fact that we are indeed working on the basis of this framework, as was broadly acknowledged during our previous sessions. This was also done in para 8 of the 2021 OEWG report.

Text proposal for para 1

1. The first, second and third substantive sessions of the Open-ended Working Group (OEWG) on the security of and in the use of Information and Communications Technologies (ICTs) 2021-2025 took place in a challenging geopolitical environment with rising concern over the malicious use of ICTs by State and non-state actors against critical infrastructure and essential services, including in the context of armed conflict. At these sessions, States recalled the contributions on this issue by of the first OEWG on this issue, established pursuant to General Assembly Resolution 73/27, which concluded its work in 2021, and the Group of Governmental Experts established pursuant to General Assembly Resolution 73/266, which concluded their work in 2021. Furthermore, States reaffirmed the consensus report of the 2021 OEWG on developments in the field of ICTs in the context of international security\(^1\) and the consensus reports of the 2010, 2013, 2015, and 2021 groups of governmental experts (GGEs).\(^2\) States recalled and reaffirmed that the reports of these Groups “recommended 11 voluntary, non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time”, and that “specific confidence-building, capacity-building and cooperation measures were recommended”. States also recalled and reaffirmed that “international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment”\(^3\). These elements consolidate an
initial framework for responsible State behaviour in the use of ICTs providing a foundation upon which the OEWG builds its work. States also recalled the consensus resolutions of the General Assembly in which States agreed they should be guided in their use of ICTs by the OEWG and GGE reports.

**Paragraph 3**

Comments
- [Paragraph 3, final sentence]: we have had long discussions on the modalities for multi-stakeholder participation. As the sentence indicates, there were indeed many views expressed, it may be difficult to capture those views in a sentence that all of us are comfortable with. We therefore support EU’s proposal to delete this sentence.

**Textual Proposal for final text paragraph 3**

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.

**Paragraph 5**

Comments
- We welcome the reference to women’s participation and gender in this new paragraph. Gender is part of our mandate in line with resolution 1325. 1325 a landmark Security Council resolution that urges all actors to increase the participation of women and incorporate gender perspectives in all UN peace & security efforts.
B. Existing and Potential Threats

Paragraph 7

Comments

- On the threat section: A common understanding of the threats we are seeking to address is a vital element of our work. And the threat picture has evolved since the adoption of the 2021 OEWG and GGE reports. Our concern over the military use of ICTs in the context of an armed conflict has materialized, while we increasingly see issues such as ransomware have impacts on critical infrastructure and essential services.

- The current list of measures to address threats all have place in other parts of the report.

Separately from our preference to have a descriptive threats section, we have several comments on the language currently included in the section:

- [Para 7a, first sentence] It is important for this group to build its work on a common understanding of the threats to international cybersecurity, so we welcome the addition of this paragraph. When recalling the threat identified previously, we ask that both the 2021 OEWG and GGE reports are referenced.

- On the list of paragraph 7b three points:

  - [para 7b, item 4] instead of using the words threat intelligence, we suggest to use threat assessments.

  - [para 7b, item 6 and 7] We consider that item 6 and 7 in this list, covering law enforcement and mutual legal assistance are in fact areas related to cybercrime, which are being actively discussed in the Ad-Hoc Committee on Cybercrime. So we request them to be deleted here.

  - [para 7b item 10] In item 10, we welcome the reference to the general availability and integrity of the internet. As an editorial point, I would request for this concept to be reflected in line with the 2021 OEWG and GGE reports. In these reports the concept is referred to as “the technical infrastructure essential to the general availability and/or integrity of the internet”.

Textual proposal for final text for paragraph 7.a

7.a.
States, recalling the threats identified in the 2021 OEWG and GGE reports, reiterating increasing concern that threats in the use of ICTs continue to intensify and evolve, and underscoring the implications of the malicious use of ICTs for the maintenance of international peace and security, proposed that the OEWG, as a UN inter-governmental body, could be a platform to foster global, inter-regional cooperative approaches on security in the use of ICTs.

Textual proposals for final text for paragraph 7.b items (iv), (vi), (vii), (x)

7.b.
(iv) Sharing of risk assessments and technical information between States including relevant threat intelligence assessments and compendiums;
(vi) Undertaking international exercises and technical training including of law enforcement officials in coordination with other relevant processes and entities; [delete]
(vii) Prioritizing mutual legal assistance in coordination with other relevant processes and entities; [delete]
(x) Measures to safeguard the technical infrastructure essential to the general availability and/or integrity of the internet.

Recommendation 2
Comment
- We welcome the sharing of threat assessments in the OEWG. However, in our view the OEWG is not a platform for intelligence sharing.

Textual proposal for recommendation 2
States consider utilizing the framework of the OEWG to further exchange technical information relating to existing and potential threats to security in the use of ICTs, including the sharing of risk assessments, relevant threat intelligence, best practices, and incident mitigation measures, on a voluntary basis.