PERMANENT MISSION OF THE REPUBLIC OF SINGAPORE
UNITED NATIONS | NEW YORK

3 March 2023

Excellency,

I have the honour of addressing you in my capacity as Chair of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG), established pursuant to General Assembly resolution 75/240 adopted on 31 December 2020.

In my letter dated 22 February 2023, I had circulated a provisional programme of work for the fourth substantive session of the OEWG that will be held from 6 to 10 March 2023. Based on feedback and reactions I have received from some delegations, I have decided to revise and simplify the provisional programme of work, in order to facilitate its smooth adoption, and to issue the Chair's guiding questions separately for delegations' reference.

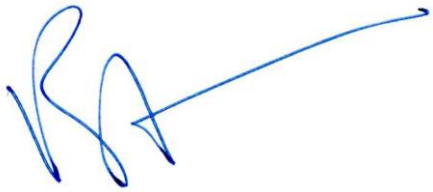
I wish to remind delegations that the programme of work is intended as a flexible tool to organize the work of the OEWG. As Chair, I will continue to be guided by the mandate of the OEWG as well as the first Annual Progress Report, which we have all agreed will serve as a "roadmap for focused discussions on specific topics within the OEWG's mandate".

In this regard, the guiding questions are issued under my own responsibility to facilitate focused discussions and seek the views of delegations on very specific issues. The guiding questions are non-exhaustive and do not seek to constrain or limit our discussions. As we seek to address the various issues under the mandate of the OEWG, it is important that we proceed in an incremental and step-by-step manner, in order to build convergence on as many issues as possible.

318 East 48th Street, New York, NY 10017, United States of America | T +1 (212) 826 0840 F +1 (212) 826 2964 | mfa.gov.sg/newyork

I would like to thank all delegations for their commitment to meaningful and constructive engagement within the OEWG, and I look forward to working closely with all of you at the fourth substantive session of the OEWG, in accordance with the mandate of the OEWG and the first Annual Progress Report.

Please accept, Excellency, the assurances of my highest consideration.



Burhan Gafoor
Chair
Open-Ended Working Group on
security of and in the use of
information and
communications technologies
2021-2025

All Permanent Representatives and Permanent Observers to the United Nations
New York

Enclosure:

- Annex A – Revised Provisional Programme of Work for the Fourth Substantive Session
- Annex B – Chair's Guiding Questions for Focused Discussions, taking into account General Assembly Resolution 75/240 and the First Annual Progress Report (A/77/275)

Annex A

Revised Provisional Programme of Work

Monday, 6 March

10 a.m.-1 p.m.

Opening of the session

Opening statements

- Ms. Izumi Nakamitsu, Under-Secretary-General and High Representative for Disarmament Affairs
- H.E. Ambassador Burhan Gafoor, Chair of the Open-ended working group on security of and in the use of information and communications technologies 2021-2025

Agenda item 3: Organization of work

Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240[1]

Continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats [from para 1, GA resolution 75/240]

3-6 p.m.

Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240

Further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour [from para 1, GA resolution 75/240]

[1] **States are strongly encouraged to use their interventions under each sub-agenda item, under "Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240", to focus on the specific topics and discussion points identified for follow-up in the Working Group's first annual progress report as contained in A/77/275.**

Tuesday, 7 March

10 a.m.-1 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *Further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour [from para 1, GA resolution 75/240]*
3-6 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *How international law applies to the use of information and communications technologies by States [from para 1, GA resolution 75/240]*

Wednesday, 8 March

10 a.m.-1 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *Confidence-building measures [from para 1, GA resolution 75/240]*
3-6 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *Confidence-building measures [from para 1, GA resolution 75/240]*

Thursday, 9 March

10 a.m. -1 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *Capacity-building [from para 1, GA resolution 75/240]*
3-6 p.m.	**Informal, dedicated stakeholder segment** *Capacity-building [from para 1, GA resolution 75/240]*

Friday, 10 March

10 a.m. -1 p.m.	**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** *Establish, under the auspices of the United Nations, regular, institutional dialogue with the broad participation of States [from para 1, GA resolution 75/240]*
3-6 p.m.	**Agenda item 6: Other matters** **Closing of the session** Concluding remarks by the Chair

ANNEX B

CHAIR'S GUIDING QUESTIONS FOR FOCUSED DISCUSSIONS, TAKING INTO ACCOUNT GENERAL ASSEMBLY RESOLUTION 75/240 AND THE FIRST ANNUAL PROGRESS REPORT (A/77/275)

Existing and Potential Threats

Chair's guiding questions for a focused discussion on threats identified in paragraphs 8 to 13 of the 2022 Annual Progress Report (APR):

- Paragraph 11 of the Annual Progress Report refers to new and emerging technologies whose properties and characteristics can create "new vectors and vulnerabilities that can be exploited for malicious ICT activity". What are these new and emerging technologies and how are they exploited for malicious ICT activity? How can the international community collectively develop a deeper understanding of their potential risks?

- What concrete, specific initiatives can States and other interested parties undertake within the framework of the OEWG to mitigate the impact of new and emerging ICT threats on international security?

- Which technical developments have States identified as contributing to emerging and potential threats, inter alia those referenced in paragraphs 8 to 13? (e.g. proliferation of marketplaces for zero-day exploits, systemic effects of vulnerabilities in widely used open-source software). What further measures can be undertaken by States to reduce the risk to international security posed by such developments?

- In light of existing and potential threats identified by States, including those referenced in the APR, what specific capacities would States require to (a) support implementation of the framework for responsible State behaviour in the use of ICTs; and/or (b) develop an adequate security infrastructure to mitigate these threats in ICT security?

Rules, Norms and Principles of Responsible State Behaviour

Chair's guiding questions for a focused discussion on non-exhaustive list of proposals annexed to the Chair's Summary of the 2021 OEWG report:

- Are there any suggestions for updates or further elaboration to the non-exhaustive list of proposals annexed to the Chair's Summary in the 2021 OEWG Report, in light of further discussions that have taken place within the OEWG since then?

- Which of these proposals ought to be developed further so as to be incorporated into future Annual Progress Reports of the OEWG?

- What can be done to help facilitate a deeper discussion on these proposals so as to achieve the potential attainment of consensus on some or all of these?

Chair's guiding questions for a focused discussion on development of guidance, checklists and sharing of national views on technical ICT terms:

- Which topics should be most urgently examined in the context of developing guidance and/or checklists so as to facilitate developing common understandings on rules, norms and principles of responsible State behaviour in the use of ICTs?

International Law

Chair's guiding questions for a focused discussion, as a starting point, on a first cluster of issues identified in the APR, namely: How international law, in particular the Charter of the United Nations applies in the use of ICTs; sovereignty; sovereign equality; non-intervention in the internal affairs of other States; and peaceful settlement of disputes:

- What are the existing legal frameworks that may be relevant to the regulation of States' conduct in cyberspace? Are there any gaps in such legal frameworks with regard to the regulation of States' conduct in cyberspace and if so, how should they be addressed?

- What types of capacities are needed to bolster States' understandings on how international law applies in the use of ICTs?

- How can we increase States' capacity thresholds in these areas, and to this end, what resources and institutional support etc. are needed?

<u>Confidence-Building Measures</u>

Chair's guiding questions for a focused discussion on revised Chair's Elements Paper for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory:

- [Please refer to Chair's revised non-paper dated 28 February 2023]

Chair's guiding questions for a focused discussion on topics which could support and foster confidence-building:

- What concrete, specific CBMs are currently in place at the (sub-)regional level in the ICT security domain that could be expanded to the global, inter-governmental context?

- Are there concrete, specific CBMs currently in place within other domains in the field of international security that could be adapted to the domain of ICT security?

- What further measures (if any) can be taken by States and/or the OEWG to better utilise existing resources and platforms to promote increased confidence and transparency between States?

Capacity-building

Chair's guiding questions for a focused discussion to exchange views and ideas on capacity-building efforts on security in the use of ICTs, leveraging on existing initiatives:

- Are there concrete, specific capacity-building mechanisms currently in use within other UN fora that could potentially be adapted to the ICT security domain?

- How can the OEWG best leverage existing capacity-building initiatives in the area of security of and in the use of ICTs? What are the potential opportunities for synergy and coordination among existing initiatives? Are there gaps that need addressing?

Chair's guiding questions for a focused discussion on funding specifically for capacity-building efforts on security in the use of ICTs through potential coordination and integration with existing development programmes and funds:

- Are there existing funding mechanisms that could be leveraged for capacity-building in the area of security of and in the use of ICTs?

- How can the States and the OEWG work together with those development programmes and funds to unlock greater access to capacity-building for developing countries?

Chair's guiding questions for a focused discussion on best practices and lessons learnt on the topic of public-private partnerships for capacity-building in the area of security in the use of ICTs:

- Are there good examples of public-private partnerships on capacity-building in the area of security of and in the use of ICTs?

- Are there lessons that can be gleaned from those examples?

Regular Institutional Dialogue

Chair's guiding questions for a focused discussion on key principles in the design of regular institutional dialogue:

- In considering regular institutional dialogue on the topic of ICT security within the UN, what are the key principles that need to be considered in their design?

- How do we ensure that discussions on ICT security at the UN continue in an inclusive manner, with the broad participation of all Member States?

. . . . .