United Nations A/AC.292/2023/2

General Assembly

Distr.: General
23 February 2023

Original: English

Open-ended working group on security of and in the use of information and communications technologies 2021–2025
Fourth substantive session
New York, 6–10 March 2023

Provisional programme of work

Note by the Secretariat

1. The fourth substantive session of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, established pursuant to General Assembly resolution 75/240, will be held at Headquarters from 6 to 10 March 2023.

2. The provisional programme of work of the fourth substantive session is contained in the annex to the present note. The annotated agenda for the session, as adopted by the working group at its organizational meeting on 1 June 2022, is contained in document A/AC.292/2021/1.

3. Additional information can be found at https://meetings.unoda.org/open-ended-working-group-information-and-communication-technologies-2021.

23-03377 (E) 270223

Annex

Provisional programme of work

Date/time	*Agenda item/programmme*
Monday, 6 March	
10 a.m.–1 p.m.	**Opening of the session**
	Opening statements
	– Under-Secretary-General and High Representative for Disarmament Affairs, Izumi Nakamitsu
	– Chair of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, Burhan Gafoor
	Agenda item 3: organization of work
	Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240[1]
	(d) 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
	Focused discussion on threats identified in paragraphs 8 to 13 of the 2022 annual progress report (as contained in document A/77/275):
	• New and emerging technologies whose properties and characteristics can create new vectors and vulnerabilities that can be exploited for malicious information and communications technology (ICT) activity (see A/77/275, para. 11). 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 open-ended working group 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, including those referenced in paras. 8 to 13 of document A/77/275? For example, the proliferation of marketplaces for zero-day exploits, and the 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?

[1] States are strongly encouraged to use their interventions under each agenda sub-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 document A/77/275.

Date/time	*Agenda item/programmme*
	• In the light of existing and potential threats identified by States, including those referenced in the report, what specific capacities would States need in order: (a) to support implementation of the framework for responsible State behaviour in the use of ICT; and/or (b) to develop an adequate security infrastructure to mitigate these threats in ICT security?
3–6 p.m.	**Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** (a) 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 Focused discussion on the non-exhaustive list of proposals contained in the Chair's summary (see A/75/816, annex II): • Are there any suggestions for updates to or further elaboration of the non-exhaustive list of proposals, in the light of further discussions that have taken place within the open-ended working group since then? • Which of these proposals should be developed further so as to be incorporated into future annual progress reports of the open-ended working group? • 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?
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** (a) 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 (*continued*) Focused discussion on the 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 the development of common understandings on rules, norms and principles of responsible State behaviour in the use of ICT?
3–6 p.m.	**Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** (e) How international law applies to the use of information and communications technologies by States

Date/time	*Agenda item/programmme*
	Focused discussion, as a starting point, on a first cluster of issues identified in the annual progress report, namely, how international law, in particular the Charter of the United Nations, applies in the use of ICT; sovereignty; sovereign equality; non-intervention in the internal affairs of other States; and peaceful settlement of disputes: • What existing legal frameworks 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 ICT? • How can we increase States' capacity thresholds in these areas and, to that end, what resources and institutional support, etc., are needed?
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** (f) Confidence-building measures Focused discussion on the revised chair's elements paper for the development and operationalization of a global, intergovernmental points of contact directory
3–6 p.m.	**Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** (f) Confidence-building measures (*continued*) Focused discussion on topics that could support and foster confidence-building: • What concrete, specific confidence-building measures are currently in place at the regional and subregional levels in the ICT security domain that could be expanded to the global, intergovernmental context? • What concrete, specific confidence-building measures are 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 open-ended working group to better utilize existing resources and platforms to promote increased confidence and transparency between States?

Date/time	*Agenda item/programmme*
Thursday, 9 March	
10–11.30 a.m.	**Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** (g) Capacity-building Focused discussion to exchange views and ideas on capacity-building efforts on security in the use of ICT, leveraging existing initiatives: • What concrete, specific capacity-building mechanisms are currently in use within other United Nations forums that could potentially be adapted to the ICT security domain? • How can the open-ended working group best leverage existing capacity-building initiatives in the areas of ICT security and use? What are the potential opportunities for synergy and coordination among existing initiatives? Are there any gaps that need to be addressed?
11.30 a.m.–1 p.m.	**Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** (*continued*) (g) Capacity-building (*continued*) Focused discussion on funding, specifically for capacity-building efforts on security in the use of ICT through potential coordination and integration with existing development programmes and funds: • What existing funding mechanisms could be leveraged for capacity-building in the areas of ICT security and use? • How can States and the open-ended working group work together with those development programmes and funds to unlock greater access to capacity-building for developing countries?
3–6 p.m.	**Informal, dedicated stakeholder segment** Focused discussion on best practices and lessons learned on the topic of public-private partnerships for capacity-building in the areas of ICT security and use: • What good examples are there of public-private partnerships on capacity-building in the areas of ICT security and use? • What lessons can be gleaned from those examples?
Friday, 10 March	
10–11.30 a.m.	**Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** (c) Establish, under the auspices of the United Nations, regular, institutional dialogue with the broad participation of States

Date/time	*Agenda item/programmme*
	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 United Nations, what are the key principles that need to be considered in their design? • How do we ensure that discussions on ICT security at the United Nations continue in an inclusive manner, with the broad participation of all Member States?
11.30 a.m.–1 p.m.	**Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240** (c) Establish, under the auspices of the United Nations, regular, institutional dialogue with the broad participation of States (*continued*) Focused discussion to further elaborate the programme of action with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICT, which would, inter alia, support the capacities of States in implementing commitments in their use of ICT; and on the relationship between the programme of action and the open-ended working group, as well as the scope, content and structure of a programme of action: • In considering the proposal for a programme of action with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICT, how do States understand its relationship with the open-ended working group? • In what specific ways can the programme of action complement the ongoing work of the open-ended working group?
3–6 p.m.	**Agenda item 6: other matters** **Closure of the session** Concluding remarks by the Chair