7 March 2022

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.

The second substantive session of the OEWG will be held at the United Nations Headquarters in New York from 28 March to 1 April 2022. The meeting will be held in-person and will also be webcast on UN WebTV. Information regarding meeting rooms will be communicated in due course by the Secretariat.

The programme of work for the second substantive session, structured in line with the agenda adopted at our organizational session (A/AC.292/2021/1) and General Assembly resolution 75/240, is enclosed. For the second substantive session, I believe that we will benefit from focused discussions on proposals and suggestions that had been raised at our first substantive session in December 2021. In this regard, I have prepared a list of guiding questions, as enclosed, which I invite delegations to address in their statements.

As indicated in my letter dated 15 November 2021, I plan to engage interested stakeholders, including businesses, non-governmental organisations and academia, in a virtual informal dialogue ahead of the second substantive session on 24 March 2022. This is a follow-up meeting to the virtual informal dialogue that I held with stakeholders on 16 December 2021.

Additionally, on the afternoon of 31 March 2022, I intend to convene a virtual open-ended informal meeting open to all delegations and interested stakeholders, including businesses, non-governmental organisations and academia.
Finally, I would like to invite delegations to a virtual open-ended informal meeting on the preparations for the second substantive session on Friday, 18 March 2022 at 9.00am (New York time). The Secretariat will disseminate the link for the meeting in due course.

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

Enclosures:
- Annex A – Provisional programme of work for the second substantive session
- Annex B – Narrative summaries of previous discussions and list of guiding questions for the second substantive session
Annex A

Provisional Programme of Work\textsuperscript{1}

Monday, 28 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

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

- Initiatives of States aimed at ensuring security in the use of
  information and communications technologies

3-6 p.m. Agenda item 5: Discussions on substantive issues contained in
paragraph 1 of General Assembly resolution 75/240 (continued)

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
(continued)

- Initiatives of States aimed at ensuring security in the use of
  information and communications technologies

\textsuperscript{1} To be issued as document A/AC.292/2022/3.
Tuesday, 29 March

10 a.m.-1 p.m.  

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

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

- Initiatives of States aimed at ensuring security in the use of information and communications technologies

3-6 p.m.  

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

How international law applies to the use of information and communications technologies by States

- Initiatives of States aimed at ensuring security in the use of information and communications technologies
Wednesday, 30 March

10 a.m.-1 p.m.  
**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)**

Confidence-building measures

- Briefing by the United Nations Institute for Disarmament Research (UNIDIR) on the UNIDIR Cyber Policy Portal (15 mins)
- Initiatives of States aimed at ensuring security in the use of information and communications technologies

3-6 p.m.  
**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)**

Confidence-building measures *(continued)*

- Initiatives of States aimed at ensuring security in the use of information and communications technologies

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

Capacity-building

- Initiatives of States aimed at ensuring security in the use of information and communications technologies
Thursday, 31 March

10 a.m.-1 p.m.  
**Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)**

Capacity-building (*continued*)

- Initiatives of States aimed at ensuring security in the use of information and communications technologies

3-6 p.m.  
**Virtual open-ended informal meeting, open to all delegations and interested stakeholders**
Friday, 1 April

10 a.m.-1 p.m. **Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)**

Establish, under the auspices of the United Nations, regular, institutional dialogue with the broad participation of States

- Initiatives of States aimed at ensuring security in the use of information and communications technologies

3 p.m.-6 p.m. **Agenda item 6: Other matters**

- Initial discussion on content and structure of annual progress report

**Closing of the session**

- Concluding remarks by the Chair

**Note:** Delegations can choose to make group or national statements in-person, in written form, or by submitting pre-recorded video statements. A link and instructions for uploading pre-recorded statements will be shared with delegations via email by the Secretariat. Delegations that intend to submit pre-recorded video statements may contact the Secretariat for support (Ms. Katherine Prizeman, Office for Disarmament Affairs, prizeman@un.org).
I 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

- At the first substantive session, States addressed a range of existing and potential threats in the sphere of information security and possible cooperative measures to prevent and counter such threats. States variously addressed many of the threats identified in the 2019-2021 OEWG consensus final report. Many States expressed concern over ICT threats posed to critical infrastructure, including critical information infrastructure. In this context, several States highlighted the vulnerability of the healthcare sector, especially against the backdrop of the COVID-19 pandemic, and noted increased challenges posed by ICT threats to the delivery of essential services. States highlighted other existing and potential threats, *inter alia*, those related to ransomware, misinformation, data security, criminal and terrorist use of ICTs, and exploitation of ICT product vulnerabilities. In exchanging views on cooperative measures to address such threats, States discussed a range of potential actions, such as tailored capacity-building efforts, including in the area of cyber hygiene, Computer Emergency Response Teams (CERTs) and Cybersecurity Incident Response Teams (CSIRTS), as well as the identification of national points of contact for both policy and technical matters.

**Suggested guiding questions:**

1. What preventative and response measures can States consider implementing in response to the potential threats identified in the first substantive session?

2. How can States enhance protection of critical infrastructure, including critical information infrastructure, from existing and potential threats?

3. How can States work together to share best practices with regard to critical infrastructure protection, at the bilateral, regional, and global levels.

---

1 The non-exhaustive narrative summaries and guiding questions provided in this document are drafted under the Chair’s sole responsibility and seek to provide States with food-for-thought in preparing for the second substantive session of the OEWG. The narrative summaries and guiding questions are not intended to limit the scope of interventions to be made by States at the second substantive session, but rather are intended to support concrete, action-oriented discussions.
4. How can States work together to share new information on existing and potential threats in real-time?

II 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

At the first substantive session, States considered rules, norms and principles of responsible State behaviour, including means of implementation and the possibility of further elaboration of rules, norms and principles. Several States noted the value of a national survey of implementation and of sharing experience and good practice in this context. States noted specific measures in support of norm implementation, *inter alia*, adoption of national legislation and establishment of CERTs. Some States called for the further development of guidance on norm implementation. Some States noted the role of regional organizations in norms implementation and others underscored the need for a mechanism to map implementation, experiences and good practices. Some States expressed the view that the existing, agreed norms could be updated and refined, while some States called for consideration of a legally binding instrument.

**Suggested guiding questions:**

1. What specific actions can the OEWG take to support concrete, practical implementation of the agreed normative framework?

2. Are there specific proposals to facilitate the implementation of the agreed normative framework which the OEWG can consider adopting? Are there any existing national/regional initiatives which the OEWG can consider expanding?

3. Are there gaps in the framework and how would they be best filled, i.e. through further elaboration of the existing norms or consideration of new ones? If the latter, which specific areas should be considered?

4. Are there any rules, norms and principles within the existing normative framework which can currently be further elaborated in specific ways?
III How international law applies to the use of information and communications technologies by States

At the first substantive session, States reaffirmed the applicability of international law, in particular the United Nations Charter, to the use of ICTs by States and supported further study of this topic. Some States referred to specific principles of international law that could be the subject of further discussion, *inter alia*, due diligence, peaceful settlement of disputes, State sovereignty and State responsibility. Other States supported discussion of the principles of international humanitarian law and human rights. Several States highlighted the importance of sharing national views on the applicability of international law with some noting the value of the Cyber Policy Portal of the United Nations Institute for Disarmament Research (UNIDIR) in this context.

**Suggested guiding questions:**

1. How can the OEWG support the sharing of national views on this topic with a view to building common understandings?

2. How can the OEWG support States’ efforts to build capacity in the areas of international law, national legislation and policy?
IV  Confidence-building measures

At the first substantive session, States exchanged views on confidence-building measures, noting specific measures that could support trust, predictability, and stability in the use of ICTs by States. Such measures included, *inter alia*, exchange of experience, including through bilateral information-sharing, (sub-) regional initiatives, identification and establishment of national points of contact, issuance of declaratory statements supporting the existing normative framework, and mechanisms for national reporting. Some States noted the importance of cross regional exchanges and of engaging with (sub-) regional organisations. Some States also noted the possibility of public-private partnerships. Additionally, some States spoke positively of the UNIDIR Cyber Policy Portal and highlighted its role in facilitating the sharing of information. Building on the conclusions of the previous OEWG, many States also specifically expressed support for the introduction of a global points of contact directory.

**Suggested guiding questions:**

1. How can the OEWG substantively engage with (sub-) regional organizations to learn from their experiences with regard to confidence-building measures?

2. How can the OEWG facilitate cross regional exchange of ideas, experiences and best practices in the development and implementation of confidence-building measures?

3. Are there examples of confidence-building measures at the (sub-) regional level that could be expanded to the global level?

4. Are there existing confidence-building measures in the field of international security that could be adapted to this context?

5. Are new confidence-building measures required and, if yes, which ones and how might they be most efficiently established?

6. How can confidence-building measures help facilitate consultation and discussion between States in uncertain or unexpected situations?

7. How can Member States and/or the OEWG better utilise the UNIDIR Cyber Policy Portal as a means to promote increased confidence and transparency between Member States?

**Proposed Global Points of Contact Directory**

8. What principles should guide the development and operationalisation of a global points of contact directory? *Inter alia*: What information should the directory...
contain? How often should the information be updated? What skills/competencies should nominated points of contact possess? What potential risks exist and how can they be mitigated? What measures can be put in place to track and ascertain the effective functioning of the directory?

9. Would further study on specific aspects of this proposal on the part of the Secretariat or other UN body (e.g. UNIDIR) be useful? If so, what specific areas of study should be considered?

10. How might the OEWG, the Secretariat and/or the UN support the establishment and maintenance of a global points of contact directory?
V Capacity-building

- At the first substantive session, States emphasized the critical importance of capacity-building in ensuring a safe, secure, peaceful and sustainable ICT environment. Underscoring the principles and processes outlined by the 2019-2021 OEWG’s consensus report, many States noted that capacity-building efforts should be objective, sustainable and results-driven. States considered specific areas of capacity-building, *inter alia*, norm implementation, cyber hygiene, establishment of national strategies, international law, incident response, emergency management and protection of critical infrastructure. Some States also noted the importance of gender-sensitive capacity-building and the role of the private sector in supporting capacity-building.

Suggested guiding questions:

1. Noting that a significant amount of capacity-building currently occurs at the (sub-)regional level, what unique roles can the UN take on to support and/or facilitate capacity-building at the global level?

2. What measures can be put in place to facilitate effective consideration of the needs of developing countries in the design and development of capacity-building measures?

3. Are there existing mechanisms for capacity-building measures in the field of international security that could be adapted to this context? Are there useful lessons the OEWG can draw from these existing mechanisms?

4. What can the OEWG learn from the role (sub-)regional organizations currently play in capacity-building? How can the OEWG engage and/or work together such organizations to optimise global capacity-building efforts?

5. What contribution can other interested stakeholders (e.g. the private sector, non-governmental organisations and academia) make to capacity-building? What mechanisms can we establish to encourage and facilitate their contribution to capacity-building in a meaningful way?

6. What can the OEWG do to support more coordinated, sustainable capacity-building efforts? Is there a role for the United Nations, including UNIDIR, in this regard?

7. What concrete measures can the OEWG, the Secretariat or other UN body take to advance capacity-building efforts in the near-to-medium term? For example, *inter alia*: Would it be useful to designate a UN cyber capacity-building focal point with the responsibility of coordinating offers and requests for capacity-building? Would it be helpful for this focal point to coordinate a calendar of capacity building programmes?
VI Establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States

- At the first substantive session, States considered the need for regular, institutional dialogue on the security of and in the use of ICTs. In this regard, several States supported regular exchange under United Nations auspices, including to support norm implementation and to build capacity. In this context, the proposal for a Programme of Action was positively referenced by many States. Many States also noted the value of inputs from academia, the private sector and civil society.

Suggested guiding questions:

1. How should a “regular, institutional dialogue” under the auspices of the United Nations be structured?

2. What distinct features should such a dialogue have, for example a list of action-oriented goals for implementation and/or a review mechanism?

3. When would be the optimal time for such a dialogue to be established?