22 February 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.

The fourth substantive session of the OEWG will be held at the United Nations Headquarters (UNHQ) in New York from 6 to 10 March 2023. The meeting will be held in-person in Conference Room 2 and webcast on UN WebTV.

In this regard, I am pleased to enclose the provisional annotated programme of work for the fourth substantive session. The programme of work has been structured such that delegations will have the opportunity to participate in focused discussions on topics under the six pillars of the Working Group’s mandate, and as identified in the first Annual Progress Report. In addition, I have also provided guiding questions relevant to each specific topic, which have been drawn from the non-exhaustive list of guiding questions earlier circulated to delegations on 22 November 2022. The aim is to help delegations identify areas of potential convergence during the focused discussions, with a view to achieving concrete and substantive outcomes or areas of progress that can be captured in our next Annual Progress Report in July 2023.

Building on the positive experience of our informal inter-sessional meetings held from 5 to 9 December 2022, I intend to allow delegations to present concept papers on specific proposals relating to the topics identified for focused discussion listed in the provisional annotated programme of work, within the constraints of available time. If your delegation intends to present new proposals or elaborate earlier proposals, please do contact the Secretariat and my team so that we can plan our work accordingly.
For the reference of delegations, I am circulating an **updated 2023 OEWG meeting schedule**, reflecting the revised dates for the fifth substantive session in July 2023. In addition, for the convenience of delegations, I am re-circulating two documents, namely (a) the **non-exhaustive list of guiding questions** issued with my letter of 22 November 2022; and (b) the **table of issues for focused discussions** at the fourth and fifth substantive session of the OEWG issued with my letter of 4 November 2022.

Finally, I would like to remind delegations that I will also be convening an **informal inter-sessional meeting** to discuss the development and operationalization of a global, intergovernmental Points of Contact directory (POC directory), which will take place **in hybrid format at 10am on 2 March 2023** (New York local time) in Conference Room 3 at UNHQ and on the Webex online platform. I am currently reviewing the comments made by delegations at the informal town hall meeting held on 15 February 2022 and am preparing a **revised version of the Chair’s non-paper** on this topic which I intend to circulate in the coming days. [Note: Information regarding hybrid connection details for the informal inter-sessional meeting will be communicated in due course by the Secretariat.]

I would like to extend my sincere appreciation once again to all delegations for your positive engagement with, and meaningful contributions to, the OEWG. I look forward to working closely with all delegations to advance the work of the OEWG at the fourth substantive session, in accordance with the mandate as established in General Assembly resolution 75/240.

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

[Signature]

**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 – Provisional Annotated Programme of Work for the Fourth Substantive Session
- Annex B – Updated 2023 OEWG Meeting Schedule
- Annex C – Non-exhaustive List of Guiding Questions
- Annex D – Table of Issues for Focused Discussions
Annex A

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

*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]*

Focused discussion on threats identified in paragraphs 8 to 13 of the 2022 Annual Progress Report:

- 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?

- *(continued on next page)*

---

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.
- 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?

**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]

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?
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]*

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?

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]*

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?
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]*

Focused discussion on revised Chair’s Elements Paper for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory

3 p.m.-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]*

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?
Thursday, 9 March

10 a.m. -11.30 a.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]*

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?

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)

*Capacity-building [from para 1, GA resolution 75/240]*

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?

3 p.m. -6 p.m. Informal, dedicated stakeholder segment

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?
**Friday, 10 March**

10 a.m.-11.30 a.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]*

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?

11.30 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]*

Focused discussion to further elaborate the PoA with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, which would *inter alia* support the capacities of States in implementing commitments in their use of ICTs; and on the relationship between the PoA and OEWG, and on the scope, content and structure of a PoA:

- In considering the proposal for a PoA with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, how do States understand its relationship with the OEWG?

- In what specific ways can the PoA complement the ongoing work of the OEWG?
3 p.m.-6 p.m.

**Agenda item 6: Other matters**

Closing of the session

Concluding remarks by the Chair
## Updated 2023 OEWG Meeting Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Meeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday, 1 March 2023, 8.30am (NY time)</td>
<td>Chair’s virtual informal consultations with Stakeholders</td>
</tr>
<tr>
<td>Thursday, 2 March 2023, 10.00am (NY time)</td>
<td>Hybrid informal inter-sessional meeting with Member States on POC directory</td>
</tr>
<tr>
<td>6-10 March 2023</td>
<td>Fourth Substantive Session of the OEWG</td>
</tr>
<tr>
<td>June 2023</td>
<td><em>Likely Informal consultations and/or inter-sessional meetings (tbc)</em></td>
</tr>
<tr>
<td>24-28 July 2023</td>
<td>Fifth Substantive Session of the OEWG</td>
</tr>
</tbody>
</table>
NON-EXHAUSTIVE LIST OF GUIDING QUESTIONS:
OEWG INFORMAL INTER-SESSIONAL MEETING¹
DECEMBER 2022

THEMATIC SESSION: GLOBAL POC DIRECTORY

Modalities for dissemination of information

- Will the directory be available via webpage (publicly available webpage or by password-protected webpage for States only), by periodic circulation via email or through other means of dissemination? What are the advantages and disadvantages of each of these modes of dissemination?

POC Information Management and capacity-building

- How many POCs should each State nominate – for example, distinct nominations for the diplomatic and technical levels? How can the nomination of global POCs be coordinated with the work of POCs at relevant regional directories and CERT organisations to build on already existing channels of communications and to avoid duplication?

- What information should be provided for each of these POCs? (e.g. Name, title/position, email, phone, preferred UN languages, availability etc.)

- How often should POC information be updated and by what means?

- What measures can be put in place to ensure that the information in the directory is accurate and updated? (e.g. periodic “ping” tests conducted by the directory manager)

- How could capacity-building initiatives be utilized to assist States in identifying and equipping POCs and also to make use of the global directory?

Policies for Use

¹ These questions have been prepared under the sole authority of the Chair as a means to support States in their preparations for the informal, inter-sessional meetings without prejudice to other views, proposals and suggestions States may wish to raise during the discussions.
• What policies (if any) shall govern communication between POCs? What lessons or models can be drawn from other POC directories such as at the regional level and CERT organisations?

• Should there be a distinction between working-level and senior-level POCs? If a distinction is made, under what circumstances may senior-level POCs be contacted?

• What policies, protocols and processes (if any) should govern the exchange of information among POCs? Can information exchanged be shared with inter alia (a) other States, (b) other non-State entities, or (c) made publicly available?

Potential activities for engagement

• What additional activities could be pursued to leverage the expertise available within the POC directory with the view of building on existing regional POC directories and CERT-to-CERT arrangements? (e.g. table-top exercises, information exchange mechanisms between policy makers and the technical community, incident response procedure?)

THEMATIC SESSION: CONFIDENCE-BUILDING MEASURES

• 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?

• Recommendation 5 under Section E (Confidence-Building Measures) of the OEWG’s first Annual Progress Report (APR) encouraged States to continue, on a voluntary basis, to share information through the report of the Secretary-General on developments in the field of ICTs in the context of international security, as well as the UNIDIR Cyber Policy portal as appropriate.

  o 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?

• Are there any concrete, specific initiatives which other interested parties, including businesses, non-governmental organizations and academia, could independently develop and implement that could contribute to confidence-building between States? (e.g. voluntary information sharing initiatives)
THEMATIC SESSION: (A) EXISTING AND POTENTIAL THREATS, AND (B) RULES, NORMS AND PRINCIPLES OF RESPONSIBLE STATE BEHAVIOUR

Existing and Potential Threats

- 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 of an adequate security infrastructure to mitigate these threats in ICT security?

Rules, Norms and Principles

- 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?

- 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?
Can and should member states continue to share national views on additional norms that could continue to be developed over time, particularly in the context of the evolving cyber landscape and ICT security environment?

What are some of the basic capacities required to implement the framework for responsible State behaviour? How can States be supported in the acquisition of those capacities?

THEMATIC SESSION: CAPACITY-BUILDING

- How can the principles of capacity-building in relation to State use of ICTs in the context of international security as adopted in the 2021 OEWG report be integrated into international and regional capacity-building efforts?

- Are there concrete, specific capacity-building mechanisms currently in use at the (sub)regional level in the ICT security domain that could potentially be expanded to the global, inter-governmental context?

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

- 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?

- 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?

- Are there good practice 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?

- How can States raise awareness of the gender dimensions of security of and in the use of ICTs and promote gender-sensitive capacity-building at the policy level as well as in the selection and operationalization of relevant projects?

THEMATIC SESSION: INTERNATIONAL LAW

- Which areas of international law and legal issues should States prioritise and how can these be examined with a view to moving towards greater convergence?
What are the existing legal frameworks that may be relevant to the regulation of States’ conduct in cyberspace? Are there any gaps in existing legal frameworks with regard to the regulation of States’ conduct in cyberspace?

- What types of capacities are needed to bolster States’ understandings on how international law applies in the use of ICTs?
  
  o How can we increase States' capacity thresholds in these areas, and to this end, what resources and institutional support, etc., are needed?

THEMATIC SESSION: 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?

- 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 ICTs, how do States understand its relationship with the OEWG? In what specific ways can the POA complement the ongoing work of the OEWG?

  . . . . .
### Table of issues for focused discussions at the fourth and fifth substantive sessions of the OEWG

<table>
<thead>
<tr>
<th>Topics for discussions at the fourth and fifth substantive sessions of the OEWG, as reflected in the recommended next steps in the Annual Progress Report.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing and Potential Threats</td>
</tr>
<tr>
<td>- “States engage in focused discussions on the existing and potential threats identified in paragraphs 8 to 13 at the fourth and fifth sessions of the OEWG.” [Existing and Potential Threats: Recommended next steps, para 2]</td>
</tr>
<tr>
<td>Rules, Norms and Principles of Responsible State Behaviour</td>
</tr>
<tr>
<td>- “States continue exchanging views at the OEWG with the aim of developing common understandings on, as well as facilitating the implementation of, rules, norms and principles of responsible State behaviour in the use of ICTs, including on best practices in this regard, and discuss the proposals from the non-exhaustive list in paragraph 14 (e) above, at the fourth and fifth sessions of the OEWG” [Rules, Norms and Principles of Responsible State Behaviour: Recommended next steps, para 1]</td>
</tr>
<tr>
<td>International Law</td>
</tr>
<tr>
<td>- “States engage in focused discussions on topics from the non-exhaustive list in paragraph 15(a)-(b) above as well as proposals contained in the 2021 OEWG report and Chair’s summary, where relevant, at the fourth and fifth sessions of the OEWG” [International Law: Recommended next steps, para 2]</td>
</tr>
<tr>
<td>Confidence-Building Measures</td>
</tr>
<tr>
<td>- “States agree to establish, building on work already done at the regional level, a global, intergovernmental, points of contact directory. At the fourth and fifth sessions of the OEWG, States to engage in further focused discussions on the development of such a directory, on a consensus basis, as well as engage in discussions on initiatives for related capacity-building, taking into account available best practices such as regional and subregional experiences where appropriate.” [Confidence-Building Measures: Recommended next steps, para 2]</td>
</tr>
<tr>
<td>- “The UN Secretariat is requested to seek views from States on the global points of contact directory, which could include”</td>
</tr>
</tbody>
</table>

---

*ANNEX D*
views on experiences at the regional and subregional levels, and produce a background information paper on these views by the end of January 2023 for consideration at the fourth session of the OEWG”. [Confidence-Building Measures: Recommended next steps, para 3]

- “The OEWG Chair is requested to convene an intersessional meeting with States, regional and subregional organizations and interested stakeholders as appropriate, including businesses, non-governmental organizations and academia, no later than the beginning of the fourth session, to discuss topics which could support and foster confidence building” [Confidence-Building Measures: Recommended next steps, para 4]

| Capacity-building | - “States engage in focused discussions at the fourth and fifth sessions of the OEWG on, inter alia, (a) funding specifically for capacity-building efforts on security in the use of ICTs through potential coordination and integration with existing development programmes and funds; (b) exchanging views and ideas on capacity-building efforts on security in the use of ICTs, leveraging on existing initiatives, and (c) best practices and lessons learnt on the topic of public-private security in the use of ICTs. Experts could be invited to make presentations on these topics to facilitate further discussion.” [Capacity-building: Recommended next steps, para 2] |
| Regular Institutional Dialogue | - “States, at the fourth and fifth sessions of the OEWG, to continue to engage in focused discussions within the framework of the OEWG to further elaborate the PoA with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, which would, inter alia, support the capacities of States in implementing commitments in their use of ICTs. At these sessions, States will also engage in focused discussions, on the relationship between the PoA and the OEWG, and on the scope, content and structure of a PoA.” [Regular Institutional Dialogue: Recommended next steps, para 2] |

...